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-004-7 AND CIP-011-3 ADDRESSING BULK ELECTRIC SYSTEM CYBER SYSTEM INFORMATION ACCESS MANAGEMENT

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

September 15, 2021

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-004-7 AND CIP-011-3 ADDRESSING BULK ELECTRIC SYSTEM CYBER SYSTEM INFORMATION ACCESS MANAGEMENT

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] the North American Electric Reliability Corporation ("NERC")[3] hereby submits for Commission approval proposed Reliability Standards CIP-004-7 – Cyber Security – Personnel & Training and CIP-011-3 – Cyber Security – Information Protection. The proposed Reliability Standards improve the reliability of the Bulk Electric System ("BES") by clarifying the protections required regarding use of third-party solutions for BES Cyber System Information ("BCSI"). NERC requests that the 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 G); and the retirement of currently effective Reliability Standards CIP-004-6 and CIP-011-2.

---

1 16 U.S.C. § 824o.
2 18 C.F.R. § 39.5 (2020).
3 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) [hereinafter ERO Certification Order].

As required by Section 39.5(a) of the Commission's regulations,[4] this petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit H), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[5] (Exhibit C). The NERC Board of Trustees adopted the proposed Reliability Standards on August 12, 2021.

I. SUMMARY

The suite of Critical Infrastructure Protection ("CIP") Reliability Standards require protections around BES Cyber Systems, the most critical cyber devices on the electric grid. As defined in the NERC Glossary of Terms used in Reliability Standards ("NERC Glossary"), BCSI is "[i]nformation about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."[6] Given the importance of BCSI, Responsible Entities must control access to this information. In currently effective Reliability Standards CIP-004-6 and CIP-011-2, Responsible Entities do this by managing access to the "designated storage location" of BCSI, such as an electronic document or physical file room. However, as technology has evolved, third-party services, such as cloud services, have become a viable and safe option for storing BCSI. The protections available for Responsible Entities to secure information in the cloud,

---

[4] 18 C.F.R. § 39.5(a).

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC 61,104 at PP 262, 321-37 (2006) [hereinafter Order No. 672], *order on reh'g*, Order No. 672-A, 114 FERC 61,328 (2006).

[6] The rest of the definition also states:

> BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

The NERC Glossary is available at https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

for example, depend less on the actual storage location of the information and more on file-level rights and permissions. As a result, the revisions in proposed Reliability Standards CIP-004-7 and CIP-011-3 would allow Responsible Entities to leverage these protections within their control for third-party data storage and analysis systems.

To that end, proposed CIP-004-7, which pertains to personnel and training, includes the following modifications:

- Removes references to "designated storage locations" of BCSI;
- Adds Requirement R6 regarding an access management program to authorize, verify, and revoke provisioned access to BCSI; and
- Other minor clarifications to update the standard.

Proposed Reliability Standard CIP-011-3, which pertains to information protection, includes the following modifications:

- Clarifies requirements regarding protecting and securely handling BCSI; and
- Other minor clarifications to update the standard.

The proposed Reliability Standards maintain the security objectives supported in previous versions while providing flexibility for Responsible Entities to leverage third-party data storage and analysis systems. As such, the Commission should approve the proposed Reliability Standards as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[7]

Lauren Perotti*
Senior Counsel
Marisa Hecht*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Howard Gugel*
Vice President, Engineering and Standards
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,[8] 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 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.[9] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[10] 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

---

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

[8] 16 U.S.C. § 824o.

[9] *Id.* § 824o(b)(1).

[10] *Id.* § 824o(d)(5).

United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[11]

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.[12]

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.[13] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[14] 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.[15] 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.

---

11 18 C.F.R. § 39.5(a).

12 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

13 Order No. 672 at P 334.

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

15 ERO Certification Order at P 250.

Further, a vote of stakeholders and adoption by the NERC Board of Trustees is required before NERC submits the Reliability Standard to the Commission for approval.

C. Standard Drafting Team Schedule Directive

In an order issued on February 20, 2020, the Commission directed NERC to submit an informational filing outlining the project schedules for Projects 2016-02[16] and 2019-02.[17] Pursuant to paragraph 5 of the Schedules Order,[18] the Commission stated that these schedules should include the status of the projects, interim target dates, and the anticipated filing date for new or modified Reliability Standards. In addition, the Commission directed NERC to file quarterly informational status updates, beginning in June 2020, until NERC files new or modified standards with the Commission.[19]

NERC provided the initial informational filing regarding the schedules on March 19, 2020[20] and four additional quarterly informational filings with updated schedules on June 19, 2020,[21] September 17, 2020,[22] December 15, 2020,[23] March 15, 2021,[24] and June 15, 2021.[25]

---

16 Project 2016-02 – Modifications to CIP Standards focuses on modifications to the suite of CIP Reliability Standards to incorporate applicable protections for virtualized environments.

17 *N. Am. Elec. Reliability Corp.*, "Order Directing Informational Filings Regarding NERC Standard Drafting Projects," 170 FERC ¶ 61,109 (Feb. 20, 2020) [hereinafter Schedules Order].

18 *Id.*

19 *Id.*

20 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (March 19, 2020).

21 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 19, 2020).

22 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (September 17, 2020).

23 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (December 15, 2020).

24 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (March 15, 2021).

25 NERC, *Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (June 15, 2021).

NERC also provided a supplemental informational filing on November 13, 2020.[26] This petition will conclude the updates for Project 2019-02.[27]

D. Development of the Proposed Reliability Standards

As further described in Exhibit H hereto, NERC initiated a Reliability Standard development project, Project 2019-02 BES Cyber System Information Access Management ("Project 2019-02"), and appointed a standard drafting team (Exhibit I) to develop the revisions. This project was initiated due to the work of an informal team, in collaboration with the NERC Compliance Input Working Group,[28] to review the use of encryption on BCSI and its impact on compliance with NERC Reliability Standards.

On December 20, 2019, NERC posted the initial drafts of proposed Reliability Standards CIP-004-7 and CIP-011-3 for a 45-day comment period and ballot. The initial ballot did not receive the requisite approval from the registered ballot body ("RBB"). After considering comments to the initial drafts, NERC posted second drafts of the proposed Reliability Standards for another 45-day comment period and ballot on August 6, 2020. The second drafts did not receive the requisite approval from the RBB. On March 25, 2021, NERC posted the third drafts of the proposed Reliability Standards after considering comments on the second drafts. The third drafts received the requisite approval from the RBB with an affirmative vote of 83.75 percent at 84.31 quorum for proposed CIP-004-7 and an affirmative vote of 81.39 percent at 84.62 quorum for proposed CIP-

[26] NERC, *Supplemental Informational Filing of NERC Regarding Standards Development Projects*, Docket No. RD20-2-000 (November 13, 2020).

[27] As directed, NERC will continue to file updates on Project 2016-02 until those revisions are filed in a petition for approval.

[28] The Compliance Input Working Group was a subgroup of the now-disbanded NERC Critical Infrastructure Protection Committee, a stakeholder technical committee.

011-3.[29] On June 2, 2021, NERC conducted a 10-day final ballot for the proposed Reliability Standards, which received an affirmative vote of 85.8 percent at 86.5 quorum for proposed CIP-004-7 and an affirmative vote of 83 percent at 86.81 quorum for proposed CIP-011-3.[30] The NERC Board of Trustees adopted the proposed Reliability Standards on August 12, 2021.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards would enhance reliability by providing increased options for entities to leverage third-party data storage and analysis systems in a secure manner, and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The proposed revisions clarify the protections expected when using third-party solutions (e.g., cloud services). The following section discusses the revisions to the standards:

- proposed Reliability Standard CIP-004-7 (Subsection A);
- proposed Reliability Standard CIP-011-3 (Subsection B); and
- other modifications (Subsection C).

This section concludes with a discussion of the enforceability of the proposed Reliability Standards (Subsection D).

A. Proposed Reliability Standard CIP-004-7

As in currently effective Reliability Standard CIP-004-6, proposed Reliability Standard CIP-004-7 continues to include requirements that govern personnel risk assessment, training, security awareness, and access management in support of BES Cyber System security. The

[29] The third drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

[30] The final drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

revisions in proposed CIP-004-7 include a new requirement on provisioned access to BCSI that consolidates access requirements previously spread throughout CIP-004-6. Proposed Reliability Standard CIP-004-7 includes six requirements: (1) Requirement R1 requires a Responsible Entity to implement a documented security awareness process for high and medium impact BES Cyber Systems that reinforces cyber security practices for certain personnel; (2) Requirement R2 requires Responsible Entities to implement a cyber security training program that includes the applicable requirement parts; (3) Requirement R3 requires a documented personnel risk assessment program(s); (4) Requirement R4 requires a documented access management program(s) that includes the applicable requirement parts; (5) Requirement R5 requires a documented access revocation program(s) that includes the applicable requirement parts; and (6) Requirement R6 is a new requirement that requires an access management program(s) to authorize, verify, and revoke provisioned access to BCSI that includes the applicable requirement parts.

The proposed revisions in CIP-004-7 center on removing references to "designated storage locations" and focusing the requirements on provisioned access to the BCSI, not just on where it is stored. This change permits entities to implement file-level rights and permissions, such as policy-based credentials or encryption, to manage access to BCSI. Provisioned access, while not proposed as a term in the NERC Glossary, is well understood among subject matter experts. Nevertheless, Requirement R6 clarifies that: "Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys)." For example, an individual with encrypted BCSI but no encryption key has not been granted provisioned access to that BCSI because the Responsible Entity has not taken the step to give this individual the encryption key. Furthermore, while the individual has obtained the BCSI,

the individual lacks the ability to use the BCSI without the key. Therefore, that individual does not have access to BCSI. Each Responsible Entity has its own process to grant provisioned access to individuals, and the concept of "provisioned access" in Requirement R6 is referring to the Responsible Entity's process.

Proposed CIP-004-7 includes revisions that eliminate the "designated storage locations" concept in order to facilitate more appropriate protections for using third-parties. To eliminate references to "designated storage locations," Requirement Part 4.4,[31] Part 5.3,[32] and subpart 4.1.3, from CIP-004-6 have been deleted in proposed CIP-004-7 and are incorporated into the new Requirement R6 on provisioned access, as described further below.[33] This centralizes all BCSI access requirements in the standard into one, new requirement. The proposed revised Part 4.1 with the deletion of subpart 4.1.3 reads as follows, in blackline:

> **4.1** Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
>
> **4.1.1** Electronic access; **and**
>
> **4.1.2** Unescorted physical access into a Physical Security Perimeter~~; and~~
>
> ~~**4.1.3** Access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

Proposed new Requirement R6 applies to high impact BES Cyber Systems; medium impact BES Cyber Systems with External Routable Connectivity; and Electronic Access Control or

---

[31] The deleted Part 4.4 from CIP-004-6 reads as follows: Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

[32] The deleted Part 5.3 from CIP-004-6 reads as follows: For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

[33] Requirement 5.4 in CIP-004-6 becomes Requirement 5.3 in proposed CIP-004-7 as a result of this deletion.

Monitoring Systems ("EACMS") and Physical Access Control Systems ("PACS") associated with these high and medium BES Cyber Systems. Proposed new Requirement R6 reads as follows:

> **R6.** Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information.* To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

There are three new requirement parts within Requirement R6. Proposed Part 6.1 requires Responsible Entities to authorize provisioned electronic access and provisioned physical access to BCSI. Proposed Part 6.2 incorporates into the access management program the deleted Part 4.4 obligations to verify individuals with provisioned access are still appropriate. Finally, proposed Part 6.3 incorporates into the provisioned access program the deleted Part 5.3 obligation to remove an individual's ability to use provisioned access to BCSI for a termination action. Proposed Parts 6.1, 6.2, and 6.3 provide as follows:

> **6.1** Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
>
> **6.1.1.** Provisioned electronic access to electronic BCSI; and
>
> **6.1.2.** Provisioned physical access to physical BCSI.
>
> **6.2** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:
>
> **6.2.1.** have an authorization record; and
>
> **6.2.2.** still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

6.3 For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

B. Proposed Reliability Standard CIP-011-3

Proposed Reliability Standard CIP-011-3 addresses information protection of BCSI and includes two requirements. Proposed Requirement R1 requires Responsible Entities to implement a documented information protection program(s) that includes the applicable requirement parts. Proposed Requirement R2 requires Responsible Entities to implement documented processes regarding BES Cyber Asset reuse and disposal, consistent with the applicable requirement parts. Proposed Requirement R1 includes the only substantive modifications to CIP-011-3, which are shown in blackline below:

R1. Each Responsible Entity shall implement one or more documented information protection program(s) **for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program*** that collectively includes each of the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection **Program**. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

The language added to Requirement R1 helps scope the applicability of the requirement parts to the BCSI pertaining to the systems listed in the applicability column of Table R1 – Information Protection Program. This clarifies the intent of the requirement to place protections around the BCSI, regardless of its storage location. This revision permits Responsible Entities to leverage more appropriate protections for use with third parties.

Within Requirement R1, proposed CIP-011-3 Table R1 – Information Protection Program includes two modified requirement parts. Proposed Parts 1.1 and 1.2 apply to high and medium impact BES Cyber Systems and their associated EACMS and PACS. Proposed Parts 1.1 and 1.2 provide as follows, in blackline:

1.1 Method(s) to identify **BCSI** ~~information that meets the definition of BES Cyber System Information~~.

1.2 ~~Procedure(s) for protecting and~~ **Method(s) to protect and** securely handl~~e~~**ing** **BCSI to mitigate the risks of compromising confidentiality** ~~BES Cyber System Information, including storage, transit, and use~~.

The proposed changes to Parts 1.1 and 1.2 clarify and simplify the requirement language. Proposed Part 1.1 removes redundant language. Proposed Part 1.2 includes more objective-level language to once again focus the protections on the BCSI itself. The proposed objective of Part 1.2 is "to mitigate the risks of compromising confidentiality." The intent of proposed Part 1.2 is to protect BCSI from unauthorized access no matter where the BCSI is located or its state (i.e., in storage, transit, or use). Therefore, in focusing protections on preserving confidentiality, the requirements in proposed CIP-011-3 help ensure that BCSI is protected regardless of the location of the BCSI.

C. Other Modifications

The proposed Reliability Standards also contain a number of minor modifications to align the standards with revisions to other standards or initiatives in other areas. These changes are shown in redline in Exhibit A and are summarized below.

First, the Interchange Coordinator or Interchange Authority is removed from the Applicability section of the proposed Reliability Standards. This revision is consistent with FERC-approved changes to the NERC Compliance Registry under the risk-based registration initiative.[34]

[34] *N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,213 (2015) (approving removal of the Purchasing-Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

Second, the term "Special Protection Systems" has been replaced in the Applicability section of the proposed Reliability Standards with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[35]

Third, the acronym for BES Cyber System Information, BCSI, has replaced all references to BES Cyber System Information except in certain circumstances, such as first use of the term and in headers of some tables. Responsible Entities often use the acronym BCSI when implementing these requirements. As such, the standard drafting team determined to incorporate the acronym to better reflect usage in industry.

Additionally, the proposed Reliability Standards include other minor modifications to the non-enforceable sections of the standard.

D. 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.[36] 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 G provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

---

[35] In Order No. 818, the Commission approved NERC's revised definition of the term "Remedial Action Scheme" and approved certain Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes." *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*, Order No. 818, 153 FERC ¶ 61,228 (2015).

[36] 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 24 calendar months after the effective date of the Commission's order approving the proposed Reliability Standards. The 24-month implementation period is designed to afford Responsible Entities sufficient time to implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services; establish or modify vendor relationships to ensure compliance with the new and revised requirements in proposed CIP-004-7 and CIP-011-3; and make the necessary administrative changes, such as revising their information protection programs to incorporate the new requirements.

The proposed Implementation Plan also permits Responsible Entities to elect to comply with proposed CIP-004-7 and CIP-011-3 following Commission approval but prior to the standards' effective date, provided the Responsible Entity notifies its applicable Regional Entities. Some Responsible Entities desire to use third party services for BCSI sooner than the effective date, and early adoption of CIP-004-7 and CIP-011-3 would allow Responsible Entities to implement the appropriate controls commensurate with third-party use.

VI. CONCLUSION

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

- proposed Reliability Standards CIP-004-7, and CIP-011-3, 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-004-6 and CIP-011-2, effective as proposed herein.

Respectfully submitted,

/s/ Marisa Hecht

Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: September 15, 2021

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A

Proposed Reliability Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-1

CIP-004-7
Clean

A. Introduction

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

2. **Number:** CIP-004-7

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-7.

6. **Background:** Standard CIP-004 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 common subject matter of the requirements.

   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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		Transient Cyber Assets, and with Removable Media.	
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or Dated documentation of the

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their associated:	For termination actions, revoke the individual's non-shared user accounts	An example of evidence may include, but is not limited to, workflow or sign-

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	• EACMS	(unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk	and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-2

CIP-004-7
Redline

A. Introduction

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

2. **Number:** CIP-004-7~~6~~

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~Special Protection System (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.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~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 ~~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-004-7~~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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-004-7~~6~~.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-76 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 1. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 0. EACMS; and 0. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 0. A dated listing of authorizations for BES Cyber System information; 0. Any privileges associated with the authorizations; and 0. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS; and~~ ~~PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~EACMS; and~~ ~~PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.~~	~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.~~
5.3~~4~~	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 5.1 ~~or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

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, 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 ~~the NERC~~ Reliability Standards in their respective jurisdictions.

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 E~~applicable 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 E~~The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- ~~If a Responsible E~~The 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 Enforce~~Assess~~ment Program~~cesses~~:

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.

~~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-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity ~~has~~ did not implement~~ed~~ one or more documented program(s) for access management that includes a process to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information~~	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented~~	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is~~	authorize electronic access~~,~~ or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~storage locations, privileges were incorrect or unnecessary. (4.4)~~	~~processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~	~~correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~	specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Same Day Operations and Operations Planning	Medium	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3) OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.43) OR The Responsible Entity has implemented one or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access~~,~~ or unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.45) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the	reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar~~	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances. (5.54)	~~day following the effective date and time of the termination action. (5.3)~~		
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

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

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

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

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

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

Requirement R2:

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this~~

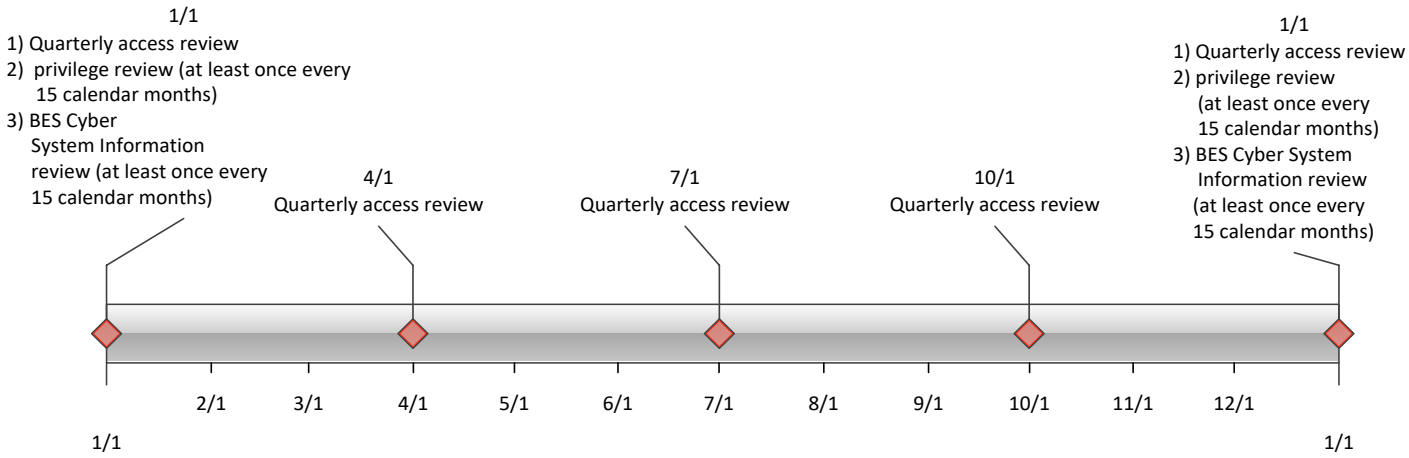
~~could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.~~

~~Requirement R4:~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~**hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.**~~

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-3

CIP-011-3
Clean

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-3

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-011-3.

6. **Background:** Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 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 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 applicable 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:

- The 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did	The Responsible Entity implemented one or more documented processes but did	The Responsible Entity has not documented or implemented any processes for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A-4

CIP-011-3
Redline

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3~~2~~

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-3~~2~~:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-3~~2~~.

6. Background:

Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify ~~information that meets the definition of BES Cyber sytem Information~~ BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify ~~BES Cyber System Information~~ BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~ BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify ~~BES Cyber System Information~~ BCSI; or • ~~Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.~~ • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	~~Procedure(s) for protecting and~~Method(s) to protect and securely handl~~e~~ing ~~BES Cyber System Information~~BCSI~~, including storage, transit, and use~~to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use ~~of BES Cyber System information~~; or • Records indicating that ~~BES Cyber System Information~~ BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-3~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain ~~BES Cyber System Information~~ BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyebr System Information~~ BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain ~~BES Cyber System Information~~BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~ BCSI prior to the disposal of an applicable Cyber Asset.

B. 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, 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 ~~the NERC~~ 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 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 applicable 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~~.~~:

~~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~~ The applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~Responsible~~ applicable ~~E~~entity is found non-compliant, it shall keep information related to the noncompliance 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 Process~~ 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- 3~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2) ~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented ~~a~~ one or more ~~BES Cyber System Information~~ BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity implemented one or more documented processes but did not include disposal or	The Responsible Entity has not documented or implemented any processes for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.1)	media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.2)	applicable requirement parts in CIP-011-3~~2~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

~~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:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~Requirement R2:~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the~~

~~analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.~~

~~Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.~~

~~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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Rationale for Requirement R2:~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of Project 2019-02 BES Cyber System Information (BCSI) Access Management is to clarify the CIP requirements related to both managing access and securing BCSI. This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

[1] See subject standards for additional information on Distribution Providers subject to the standards.

General Considerations

The 24-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011; and
- Administrative overhead to review their program.

The 24-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide Electric Reliability Organization (ERO) and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 twenty-four (24) 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 twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

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 twenty-four (24) 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 twenty-four (24) 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

Responsible Entities shall initially comply with the periodic requirements in the CIP-004-7 and CIP-011-3 within the periodic timeframes of their last performance under the CIP-004-6 and CIP-011-2.

Compliance Dates for Early Adoption of Revised CIP Standards

A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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 require Responsible Entities to manage access to BES Cyber Security Information ("BCSI") to prevent unauthorized use. To manage this access, the proposed Reliability Standards provide increased options for Responsible Entities to leverage third-party data storage and analysis systems to store BCSI in a secure manner. As a result, the proposed Reliability Standards enhance reliability by still requiring protections around access to BCSI while permitting Responsible Entities the flexibility to securely use third-party data storage and analysis systems.

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 are 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

---

1 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006) [hereinafter Order No. 672].

2 *See* Order No. 672, at P 324.

3 *See* Order No. 672, at PP 322, 325.

Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standards clearly articulate the actions that such entities must take to comply with the standard.

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 G**. 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.

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

---

4 *See* Order No. 672, at P 326.

5 *See* Order No. 672, at P 327.

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

The proposed Reliability Standards achieve the reliability goals effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standards would achieve the reliability goal of protecting BCSI through managing access to it.

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 permit Responsible Entities to leverage more types of protections to secure BCSI, including encryption.

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.

---

6 *See* Order No. 672, at P 328.

7 *See* Order No. 672, at PP 329-30.

8 *See* Order No. 672, at P 331.

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

The proposed Reliability Standards have no undue negative impact on competition. The proposed Reliability Standards require the same performance by each of the applicable Functional Entities. 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 implementation period for the proposed Reliability Standards is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop necessary processes. The proposed implementation plan also permits Responsible Entities to early adopt the revisions once approved by the Commission and upon notification of applicable Regional Entities.

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 H** 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 ballot periods. Additionally, all meetings of the drafting team

---

9 *See* Order No. 672, at P 332.

10 *See* Order No. 672, at P 333.

11 *See* Order No. 672, at P 334.

were properly noticed and open to the public. The initial and additional ballots achieved a quorum, and the last additional ballot and final ballot 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 conflict with other vital public interests.

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

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

---

[12] *See* Order No. 672, at P 335.

[13] *See* Order No. 672, at P 323.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D

Mapping Documents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D-1

Mapping Document
CIP-004-7

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 and R5 to CIP-004-X R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	CIP-004-X, Requirement R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium]*	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes clarification on the specific elements within an access management program that need to be implemented. In addition, a definition of what constitutes BCSI access was included in the parent R6 requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	[Time Horizon: Same Day Operations and Operations Planning].	
CIP-004-6, Requirement R4, Part 4.1.3 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	**CIP-004-X, Requirement R6, Part 6.1, 6.1.1, and 6.1.2** Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	The modified requirement language includes a shift from authorizing access to designated storage locations, to authorizing the provisioned access to BCSI. The Note was included to specify the type of access to be authorized (6.1), verified (6.2) and revoked (6.3).
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	**CIP-004-X, Requirement R6, Part 6.2, 6.2.1, and 6.2.2.** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is still needed.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R5, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	**CIP-004-X, Requirement R6, Part 6.3** For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.
CIP-004-6, Requirement R5, Part 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**CIP-004-6, Requirement R5, Part 5.3** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	This Part was renumbed from 5.4 to 5.3 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. The reference within the Part was changed to just Part 5.1.
CIP-004-6, Requirement R5, Part 5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the	**CIP-004-6, Requirement R5, Part 5.4** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating	This Part was renumbed from 5.5 to 5.4 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. This is a renumbering change only, no changes were made to the Part's requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D-2

Mapping Document
CIP-011-3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-X

The modifications made to requirements within CIP-011-X are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use).

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection Program*.	**CIP-011-X, Requirement R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to Applicable Systems that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program.*	Parent CIP-011-X Requirement R1 language modified to sharpen focus on protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems, which may contain BCSI.
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	**CIP-011-X, Requirement R1, Part 1.1** Method(s) to identify BCSI.	Requirement language simplified.

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	**CIP-011-X, Requirement R1, Part 1.2** Method(s) to protect and securely handle BCSI to mitigate the risks of compromising confidentiality.	Requirement revised to broaden the focus around the implementation of controls that mitigate the risks of compromising confidentiality in any state, not just storage, transit, and use.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-1

Technical Rationale
CIP-004-7

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

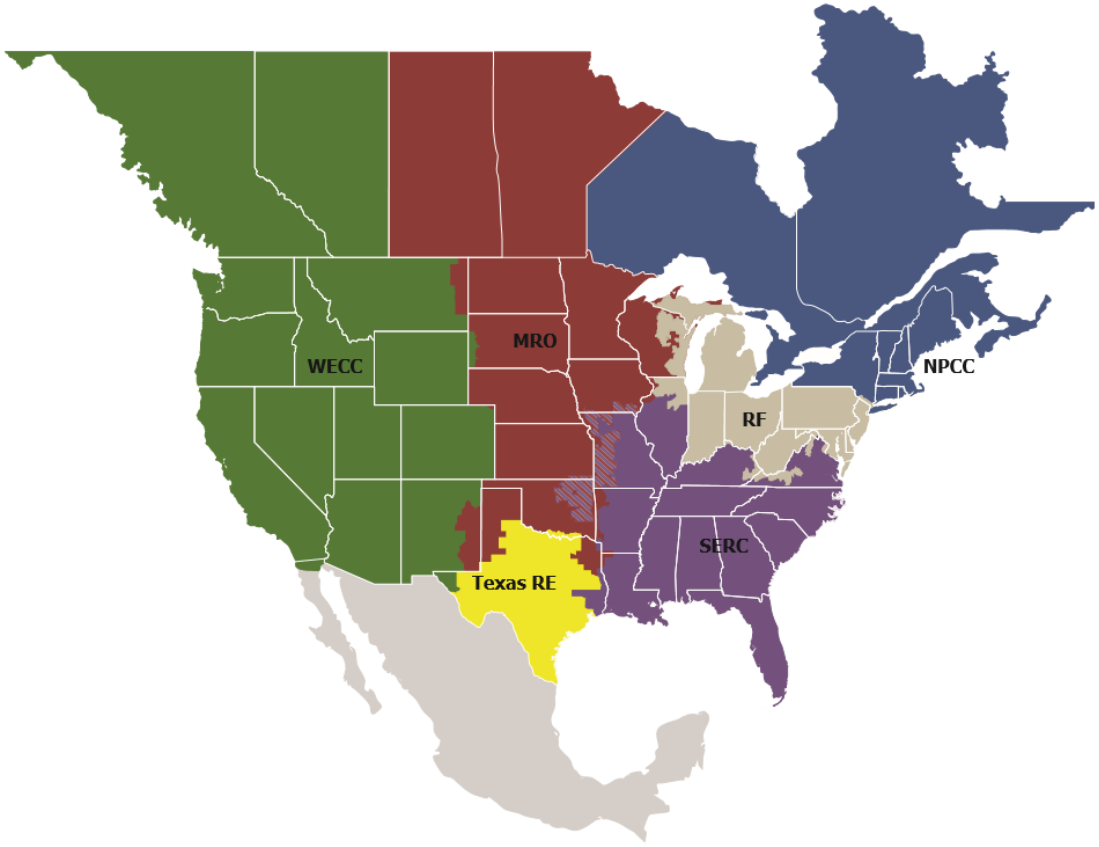
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the intent of the Standard Drafting Team (SDT) in drafting the requirements. This Technical Rationale and Justification for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving and initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT modified Reliability Standard CIP-004-X to require Responsible Entities to implement specific controls in Requirement R6 to authorize, verify, and revoke provisioned access to BES Cyber System Information (BCSI).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1

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

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

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

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

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

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

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

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals' ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have

changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.

Attachment 1: Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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

Requirement R2:
Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber

security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

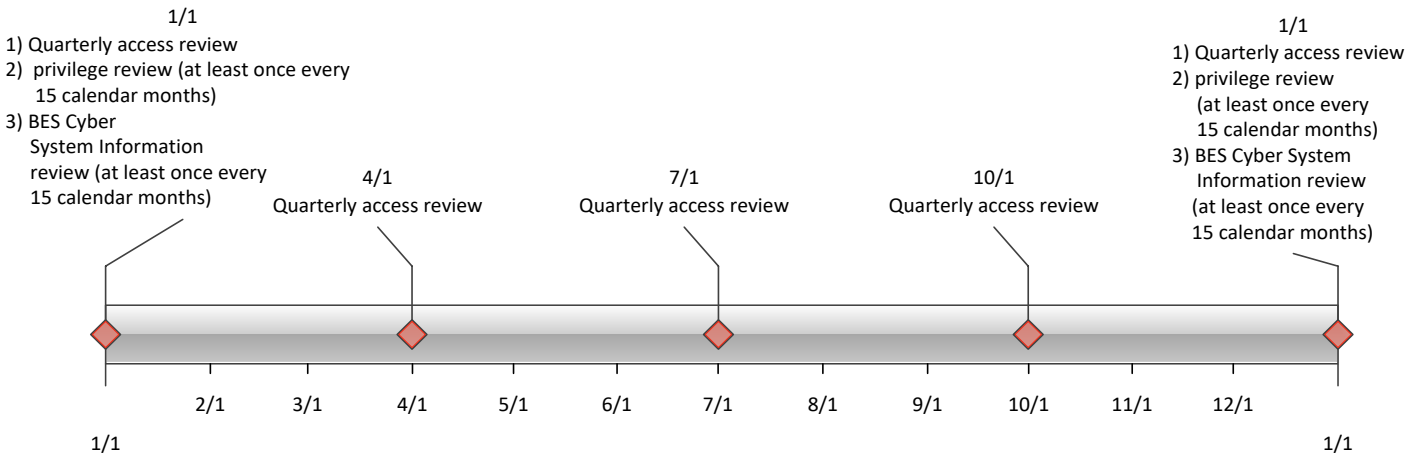
There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:
Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

An example timeline of all the reviews in Requirement R4 is included below.



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

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

Requirement R5:
The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

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

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

following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

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

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

Rationale for Requirement R5:
The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E-2

Technical Rationale
CIP-011-3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

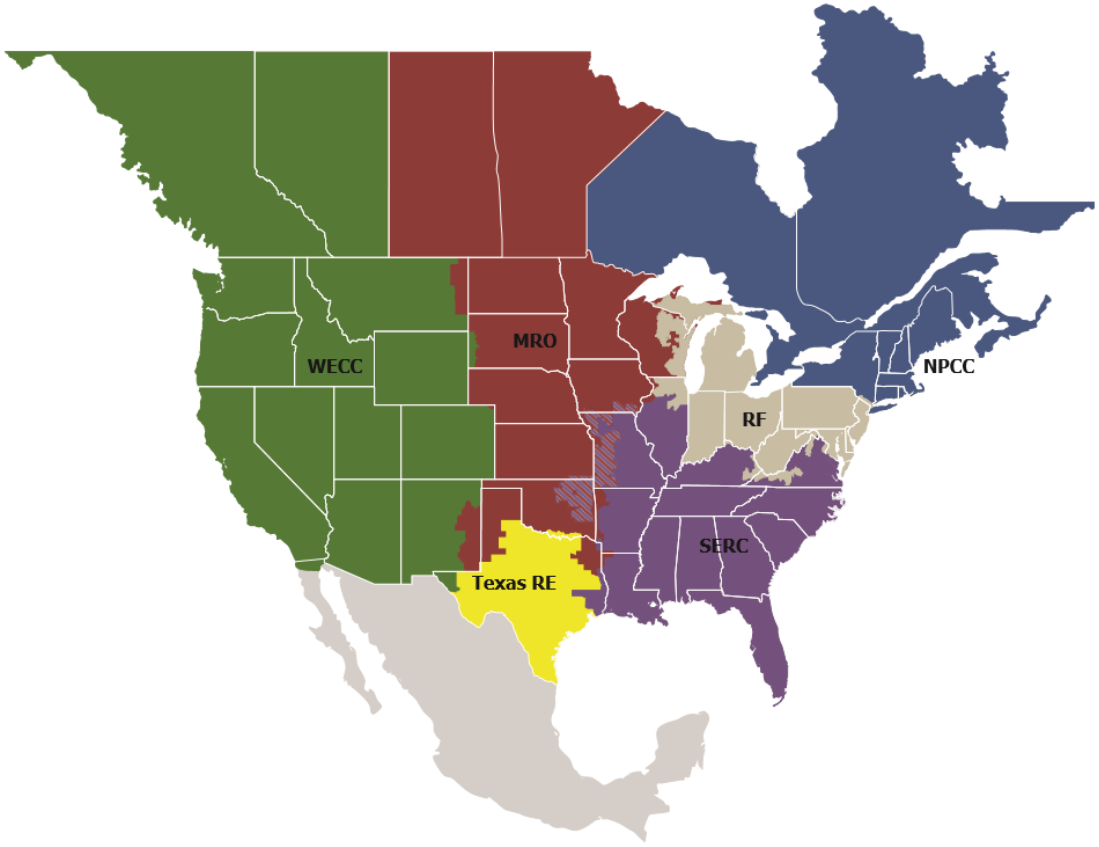
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-011-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving an initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI), by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-011-X to require Responsible Entities to implement specific methods in Requirement R1 for administrative, technical, and physical controls related to BCSI during storage, handling and use including when utilizing vendor provided cloud services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Modifications to Requirement R1:

Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1

Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Attachment 1: Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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:

Responsible Entities are free to utilize existing change management and asset management systems.
However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information. Requirement R1 Part 1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in Requirement R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal. The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.
>
> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CDRW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 of Trustees approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F

Implementation Guidance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Implementation Guidance for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

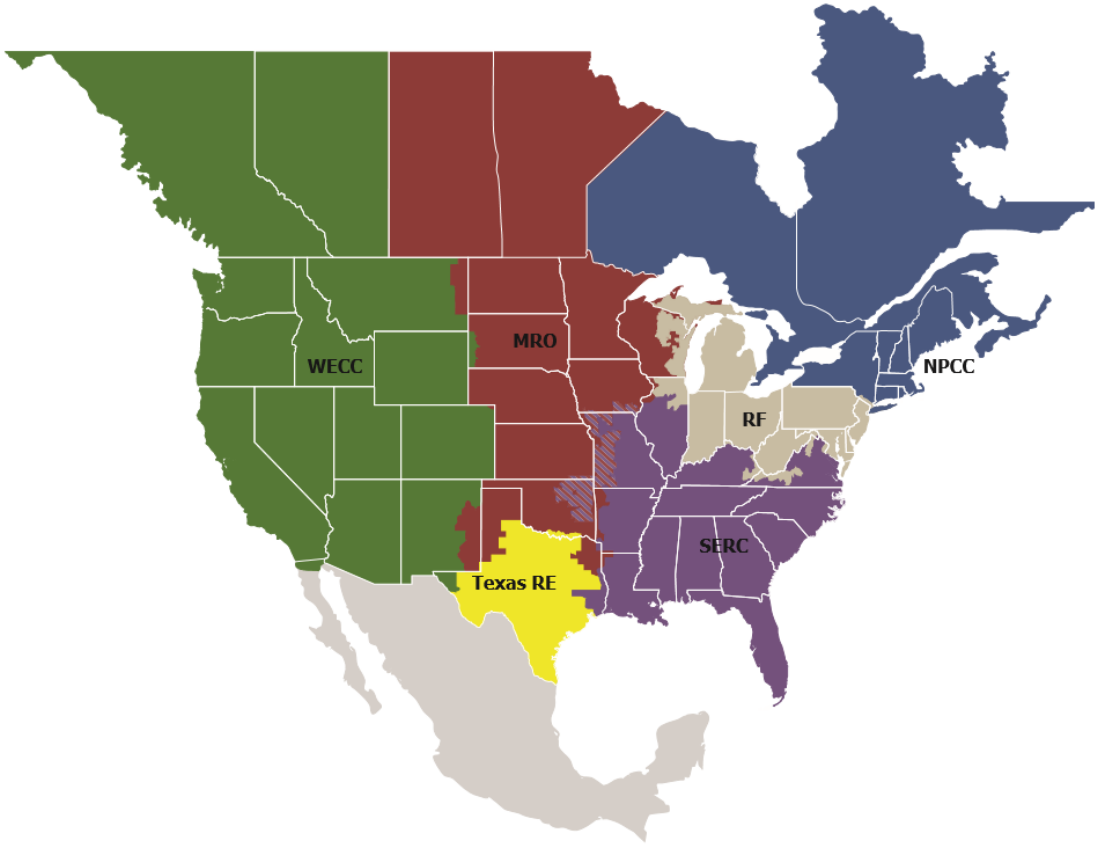
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-004-X. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for the modifications to CIP-004-X.

[1] NERC's Compliance Guidance Policy

Requirement R1

General Considerations for Requirement R1

None

Implementation Guidance for R1

None

Requirement R2

General Considerations for Requirement R2

None

Implementation Guidance for R2

The Responsible Entity has the flexibility to define the training program, and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles, or responsibilities at the discretion of the Responsible Entity.

Requirement R3

General Considerations for Requirement R3

None

Implementation Guidance for R3

None

Requirement R4

General Considerations for Requirement R4

None

Implementation Guidance for R4

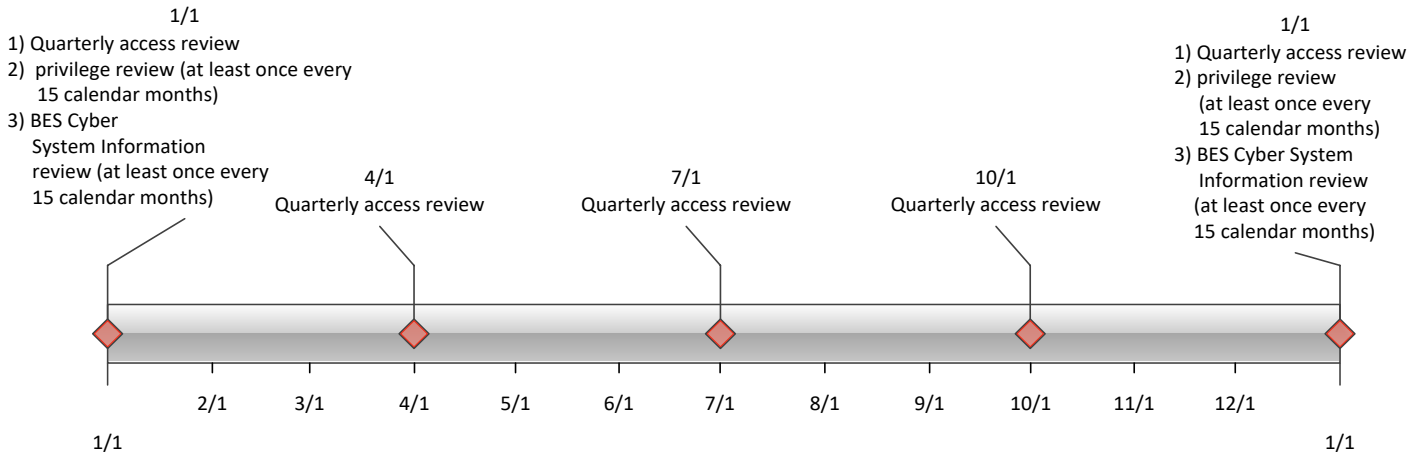
Consider including the person or persons empowered by the Responsible Entity to authorize access in the delegations referenced in CIP-003-8.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

Quarterly reviews can be achieved by comparing individuals actually provisioned access against records of individuals authorized for provisioned access. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

Entities can more efficiently perform the 15-calendar-month review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed.

An example timeline of all the reviews in Requirements R4 and R6 is included below.



Requirement R5

General Considerations for Requirement R5

None

Implementation Guidance for R5

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

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

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

If an entity considers transitioning a contracted individual to a direct hire, an entity should consider how they will meet the evidentiary requirements for Requirements R1 through R4. If evidence for compliance with Requirements R1 through R4 cannot be provided, the entity should consider invoking the applicable sub-requirements in Requirement R5 for this administrative transfer scenario. Entities should also consider including this scenario in their access management program, including a higher-level approval to minimize the instances to which this scenario would apply.

Requirement R6

General Considerations for Requirement R6

None

Implementation Guidance for R6

This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the 15-calendar-month verification in Requirement R6. The person reviewing should be different than the person provisioning access.

Entities may choose not to provision access, or provision temporary rather than persistent access, for authorized users. In other words, an authorized individual does not have to have any access provisioned, but all provisioned access must be authorized.

An entity can choose to give an authorization to access any BCSI, or they can have authorizations for specific storage locations or types of BCSI, if they so choose.

While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint

where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program. In this case, the review required in Requirement R6 Part 6.2 should still be performed, and the revocation required in Requirement R6 Part 6.3 could consist of removing the individual's name from the authorized list at the time of termination or upon review when it is determined the individual no longer has a need.

Entities can more efficiently perform the 15-calendar-month BCSI review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. For an example timeline to perform the 15-calendar-month BCSI review, refer to the graphic in the *Implementation Guidance for R4* section.

An example where a termination action in Requirement R5 Part 5.1, satisfies Requirement R6 Part 6.3, would be the Responsible Entity revoking an individual's means of unescorted physical access and Interactive Remote Access (e.g., physical access card, virtual private network, Active Directory user account). By revoking both physical and electronic access, the individual could ultimately not have access to BES Cyber System Information. The Responsible Entity should still revoke access that is manually provisioned (e.g., local user account, relay, site area network server, cloud based BCSI that is not tied to an active directory account).

Appendix 1: Implementation Guidance for CIP-004-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale sencan be found in a separate Technical Rational document for this standard.

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

Requirement R1:
Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:
The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Requirement R3:
Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check.

Requirement R4:
To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The list of provisioned individuals can be an automatically generated

account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

Requirement R5:
Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G

Analysis of Violation Risk Factors
and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G-1

Analysis of Violation Risk Factors
and Violation Severity Levels

CIP-004-7

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-7, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-7, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5
The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5
The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-7, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-7 Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified.

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-7 Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-7 R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

VSL Justifications for CIP-004-7 R6	
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 requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby 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 VSLs are based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G-2

Analysis of Violation Risk Factors
and Violation Severity Levels

CIP-011-3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-3, Requirement R1

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

The VSL justification is below.

VSLs for CIP-011-3, R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)

VSL Justifications for CIP-011-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed revisions do not lower 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 VSLs are 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 VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented information protection program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program.

VRF Justification for CIP-011-3 Requirement R2

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3 Requirement R2

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit H

Summary of Development History
and Complete Record of Development

Summary of Development History

The following is a summary of the development record for Project 2019-02 Bulk Electric System ("BES") Cyber System Information Access Management ("Project 2019-02").

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 ("SDT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the SDT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2019-02 SDT members is included in **Exhibit I**.

II. Standard Development History

A. Standard Authorization Request Development and Posting

On March 1, 2019, NERC received a Standard Authorization Request ("SAR") from Tri-State Generation and Transmission Association seeking to address BES Cyber System Information ("BCSI") access management. The SAR is the result of work by an informal team, in collaboration with the NERC Compliance Input Working Group,[3] assembled to review the use of encryption on BCSI with a particular focus on BCSI stored or used by a third party's system (i.e., the cloud). The Critical Infrastructure Protection Committee endorsed the SAR at its March 6, 2019 meeting.[4]

---

[1] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2020).

[2] The NERC *Standard Processes Manual* is available at https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/SPM_Clean_Mar2019.pdf.

[3] The Compliance Input Working Group was a subgroup of the now-disbanded NERC Critical Infrastructure Protection Committee, a stakeholder technical committee.

[4] Minutes, Critical Infrastructure Protection Committee Meeting, Agenda Item 13b.i.(1), https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC_Meeting_Minutes_March_5-6_2019.pdf.

On March 20, 2019, the Standards Committee ("SC") accepted the SAR and authorized posting it for a 30-day formal comment period and the solicitation of nominees for a SAR drafting team for a 30-day nomination period from March 28, 2019 through April 26, 2019.[5]

On May 22, 2019, the SC appointed the SAR drafting team members for Project 2019-02.[6] Based on comments received from the initial posting, the SAR drafting team made revisions to the SAR. At its July 24, 2019 meeting, the SC accepted a revised SAR, authorized drafting revisions to the Reliability Standards identified in the SAR, and appointed the SAR drafting team as the Project 2019-02 Standard Drafting Team ("SDT").[7]

At its August 21, 2019 meeting, the SC authorized posting for additional SDT members for a 30-day nomination period from August 22, 2019 through September 20, 2019.[8] On October 23, 2019, the SC appointed supplemental members to the SDT.[9] On November 20, 2019, the SC approved a final revision to the SAR.[10]

---

[5] Meeting Minutes, Standards Committee Conference Call, Agenda Item 6 (Standard Authorization Request Cyber System Information Access Management), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/Standards_Commitee_Meeting_Minutes_Approved_April_17_2019.pdf.

[6] Meeting Minutes, Standards Committee Conference Call, Agenda Item 5 (Project 2019-02 – BES Cyber System Information Access Management), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/Standards_Committee_Minutes_Approved_June_26_%202019.pdf.

[7] Meeting Minutes, Standards Committee Conference Call, Agenda Item 5 (Project 2019-02 – BES Cyber System Information Access Management), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20July%20Meeting%20Minutes_Approved_082119.pdf.

[8] Meeting Minutes, Standards Committee Conference Call, Agenda Item 6 (Project 2019-02 BES Cyber System Information Access Management), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20August%20Meeting%20Minutes_Approved_091819.pdf.

[9] Minutes, Standards Committee Meeting, Agenda Item 5 (Project 2019-02 BES Cyber System Information Access Management Supplemental SDT), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20October%20Meeting%20Minutes_Approved%20112019.pdf.

[10] Minutes, Standards Committee Meeting, Agenda Item 6a (Project 2019-02 BES Cyber System Information Access Management),

B. First Posting – Draft One of Reliability Standards and Initial Ballot

At its December 18, 2019 meeting, the SC authorized posting for a 45-day formal comment period and initial ballot.[11] The SDT posted draft one of proposed Reliability Standards CIP-004-7, CIP-011-3, an implementation plan, and other supporting materials for a 45-day formal comment period from December 20, 2019 through February 3, 2020, with an initial ballot and non-binding poll during the last 10 days from January 24, 2020 through February 3, 2020.

This posting received 91 sets of responses, including comments from approximately 209 different people from approximately 131 companies representing all 10 of the Industry Segments. Results of the initial ballot are summarized in the table below:

	Ballot	Non-binding Poll
Standard	**Quorum / Approval**	**Quorum / Supportive Opinions**
CIP-004-7	91.76% / 15.37%	88.55% / 18.88%
CIP-011-3	92.45% / 13.04%	88.21% / 15.31%
Implementation Plan	91.58% / 22.30%	

C. Second Posting – Draft Two and Second Ballot

The SDT posted draft two of proposed Reliability Standards CIP-004-7, CIP-011-3, an implementation plan, and other supporting materials for a 45-day formal comment period from

https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20November%20Meeeting%20Minutes_Approved_121819.pdf.

[11] Minutes, Standards Committee Meeting, Agenda Item 4 (Project 2019-02 BES Cyber System Information Access Management), https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20December%20Meeting%20Minutes_Approved_012220.pdf.

August 6, 2020 through September 21, 2020, with an additional ballot and non-binding poll during the final 10 days from September 11, 2020 through September 21, 2020.

This posting received 68 sets of responses, including comments from approximately 175 different people from approximately 111 companies representing all 10 of the Industry Segments. Results of the second ballot are summarized in the table below:

	Ballot	Non-binding Poll
Standard	**Quorum / Approval**	**Quorum / Supportive Opinions**
CIP-004-7	83.15% / 32.80%	80.15% / 32.08%
CIP-011-3	82.01% / 23.06%	79.47% / 24.36%
Implementation Plan	81.02% / 50.49%	

D. Third Posting – Draft Three and Third Ballot

The SDT posted draft three of proposed Reliability Standards CIP-004-7, CIP-011-3, an implementation plan, and other supporting materials for a 45-day formal comment period from

March 25, 2021 through May 10, 2021, with an additional ballot and non-binding poll during the last 10 days from April 30, 2021 through May 10, 2021.[12]

This posting received 64 sets of responses, including comments from approximately 157 different people from approximately 98 companies representing all 10 of the Industry Segments. Results of the third ballot are summarized in the table below:

	Ballot	Non-binding Poll
Standard	Quorum / Approval	Quorum / Supportive Opinions
CIP-004-7	84.31% / 83.75%	82.88% / 84.57%
CIP-011-3	84.62% / 81.39%	82.95% / 82.61%
Implementation Plan	83.64% / 92.51%	

E. Final Ballot

Final drafts of CIP-004-7, CIP-011-3, the implementation plan, and other associated documents were posted for a 10-day final ballot from June 2, 2021 through June 11, 2021.[13] Results of the final ballot are summarized in the table below:

	Ballot
Standard	Quorum / Approval
CIP-004-7	86.50% / 85.80%
CIP-011-3	86.81% / 83.00%

[12] The third drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

[13] The final drafts of the standards were posted as CIP-004-X and CIP-011-X because they were posted simultaneously with other proposed revisions to those standards as a part of Project 2016-02 Modifications to CIP Standards.

	Ballot
Standard	**Quorum / Approval**
Implementation Plan	85.87 % / 94.17%

F. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standards CIP-004-7, CIP-011-3, the implementation plan, the retirement of CIP-004-6 and CIP-011-2, and the VRFs and VSLs at its quarterly meeting on August 12, 2021.[14]

[14] NERC, *Board of Trustees Agenda Package*, Agenda Item 5a (Project 2019-02 BES Cyber System Information Access Management), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_Agenda_Package_August_12_2021_ATTENDEE.pdf.

Complete Record of Development

Project 2019-02 BES Cyber System Information Access Management

Related Files

Status

Final ballots concluded **8 p.m. Eastern, Friday, June 11, 2021** for the following:

-CIP-004-X - Cyber Security - Personnel & Training

-CIP-011-X - Cyber Security - Information Protection

-Implementation Plan

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

This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Standard(s) Affected – CIP-004-6 - Cyber Security - Personnel & Training | CIP-011-2 - Cyber Security - Information Protection

Purpose/Industry Need

The purpose of this project is to clarify the CIP requirements related to BES Cyber System Information (BCSI) access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-004-X Clean **(84)** | Redline to Last Posted **(85)** | Redline to Last Approved **(86)** Board Documents CIP-004-7 Clean **(87)** | Redline to Last Approved **(88)** CIP-011-X Clean **(89)** | Redline to Last Posted **(90)** | Redline to Last Approved **(91)** Board Documents CIP-011-3 Clean **(92)** | Redline to Last Approved **(93)** Implementation Plan **(94)** Board Implementation Plan Document **(95)** **Supporting Materials** Technical Rationale CIP-004-X **(96)** CIP-011-X **(97)** Implementation Guidance CIP-004-X **(98)** VRF/VSL Justifications CIP-004-X **(99)** CIP-011-X **(100)** Board VRF/VSL Documents CIP-004-7 **(101)** CIP-011-3 **(102)** Mapping Documents CIP-004-X Clean **(103)** | Redline **(104)** CIP-011-X **(105)**	Final Ballots Info **(106)** Vote	06/02/21 - 06/11/2021	Ballot Results CIP-004-X **(107)** CIP-011-X **(108)** Implementation Plan **(109)**	
Draft 3			Ballot Results	

CIP-004-X Clean **(59)** | Redline to Last Posted **(60)** | Redline to Last Approved **(61)** CIP-011-X Clean **(62)** | Redline to Last Posted **(63)** | Redline to Last Approved **(64)** Implementation Plan **(65)** **Supporting Documents** Unofficial Comment Form (Word) **(66)** Technical Rationale CIP-004-X **(67)** CIP-011-X **(68)** Implementation Guidance CIP-004-X **(69)** VRF/VSL Justifications CIP-004-X **(70)** CIP-011-X **(71)** Mapping Document CIP-004-X **(72)** CIP-011-X **(73)**	Additional Ballot and Non-binding Poll Updated Info **(77)** Info **(78)** Vote	04/30/21 - 05/10/21	CIP-004-X **(79)** CIP-011-X **(80)** Implementation Plan **(81)** Non-binding Poll Results CIP-004-X **(82)** CIP-011-X **(83)**	
	Comment Period Info **(74)** Submit Comments	03/25/21 - 05/10/21	Comments Received **(75)**	Consideration of Comments **(76)**
Draft 2 **CIP-004-7** Clean **(35)** | Redline to Approved **(36)** | Redline to Last Posted **(37)** **CIP-011-3** Clean **(38)** | Redline to Approved **(39)** | Redline to Last Posted **(40)** **Implementation Plan** Clean **(41)** | Redline **(42)** **Supporting Materials** Unofficial Comment Form (Word) **(43)** **Technical Rationale** CIP-004-7 **(44)** CIP-011-3 **(45)** *updated **VRF/VSL Justifications** CIP-004-7 **(46)** CIP-011-3 **(47)** **Mapping Documents** CIP-004-7 **(48)** CIP-011-3 **(49)**	Additional Ballot Info **(53)** Vote	09/11/20– 09/21/20	Ballot Results CIP-004-7 **(54)** CIP-011-3 **(55)** Implementation Plan **(56)** Non-Binding Poll Results CIP-004-7 **(57)** CIP-011-3 **(58)**	
	Comment Period Info **(50)** Submit Comments	08/06/20– 09/21/20	Comments Received **(51)**	Consideration of Comments **(52)**
Draft 1 **CIP-004-7** Clean **(14)** | Redline **(15)** *updated **CIP-011-3** Clean **(16)** | Redline **(17)**	Initial Ballot Info **(29)** Vote	01/24/20– 02/03/20	Ballot Results CIP-004-7 **(30)** CIP-011-3 **(31)** Implementation Plan **(32)**	

Implementation Plan **(18)** **Supporting Materials** Unofficial Comment Form (Word) **(19)** **Technical Rationale** CIP-004-7 **(20)** CIP-011-3 **(21)** **VRF/VSL Justifications** CIP-004-7 **(22)** CIP-011-3 **(23)** **Mapping Documents** CIP-004-7 **(24)** CIP-011-3 **(25)**			Non-binding Poll Results CIP-004-7 **(33)** CIP-011-3 **(34)**	
	Comment Period Info **(26)** Submit Comments	12/20/19– 02/03/20	Comments Received **(27)**	Consideration of Comments **(28)**
	Join Ballot Pools	12/20/19– 01/20/20		
Standard Authorization Request (SAR) Clean **(12)** | Redline **(13)**	The Standards Committee accepted the corrected SAR on November 20, 2019			
Supplemental Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(10)**	Nomination Period Info **(11)** Submit Nominations	08/22/19 - 09/20/19		
Standard Authorization Request (SAR) Clean **(8)** | Redline **(9)**	The Standards Committee accepted the SAR on July 24, 2019			
Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(6)**	Nomination Period Info **(7)** Submit Nominations	03/28/19 - 04/26/19		
Standard Authorization Request (1) **Supporting Materials** Unofficial Comment Form (Word) **(2)**	Comment Period Info **(3)** Submit Comments	03/28/19 - 04/26/19	Comments Received **(4)**	Consideration of Comments **(5)**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
While there is no direct benefit to the reliability of the BES, this initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilitzation of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (aka cloud).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements related to BES Cyber System Information access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI.			
Project Scope (Define the parameters of the proposed project):			
CIP-004 and CIP-011			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirement R4 Part 4.1.3 needs to be modified so authorization and access to BCSI is clarified to focus on the BCSI and the controls deployed to limit access. In addition, the Standard should allow multiple methods for controlling access to BES Cyber System Information, rather than just electronic and physical access to the BES Cyber System Information storage location. For example, the focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (aka cloud). As currently drafted, the requirement is focused on access to the "storage location", and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach. In addition to modifying CIP-004-6 Requirement R4 Part 4.1.3, Part 4.4, Part 5.3 and CIP-011-2 Requirement R1 should also be evaluated for any subsequent impacts to the requirements, measures and/or the guidelines and technical basis.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any iconsensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus bulding activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system (aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

Name	Company
Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC
Lonnie Ratliff	NERC
Brian Kinstad	MRO
Holly Eddy	WECC
Kenath Carver	Texas Reliability Entity, Inc.
Michael Taube	MRO
Mike Stuetzle	NPCC
Morgan King	WECC
Shon Austin	Reliability First
Tremayne Brown	SERC

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

Requested information

As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below:

EXAMPLE #1:
[Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:]
R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include:
4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.;
4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following:

- Encryption and key management,
- Physical access management,
- Electronic access management,
- Data loss prevention techniques and rights management services.

4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances;

EXAMPLE #2:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;
4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and
4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

EXAMPLE #3:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Access to electronic BES Cyber System Information.

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

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-02 BES Cyber System Information Access Management**. Comments must be submitted by **8 p.m. Eastern, April 26, 2019.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

Background Information

The purpose of this project is to clarify the CIP requirements related to BES Cyber System Information (BCSI) access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI.

The proposed scope of this project would entail modifications to CIP-004-6 and CIP-011-2. The SAR describes the proposed scope as follows:

> CIP-004-6 Requirement R4 Part 4.1.3 needs to be modified so authorization and access to BCSI is clarified to focus on the BCSI and the controls deployed to limit access. In addition, the Standard should allow multiple methods for controlling access to BES Cyber System Information, rather than just electronic and physical access to the BES Cyber System Information storage location. For example, the focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (aka cloud). As currently drafted, the requirement is focused on access to the "storage location", and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach. In addition to modifying CIP-004-6 Requirement R4 Part 4.1.3, Part 4.4, Part 5.3 and CIP-011-2 Requirement R1 should also be evaluated for any subsequent impacts to the requirements, measures and/or the guidelines and technical basis.

Questions

1. Do you agree with the proposed scope 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 SAR drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through April 26, 2019

Now Available

A 30-day formal comment period for the **Project 2019-02 BES Cyber System Information Access Management Standard Authorization Request (SAR)**, is open through **8 p.m. Eastern, Friday, April 26, 2019**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Linda Jenkins. 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. - 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 SAR 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, Latrice Harkness (via email) or at 404-446-9728.

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:	Project 2019-02 BES Cyber System Information Access Management
Comment Period Start Date:	3/28/2019
Comment Period End Date:	4/26/2019
Associated Ballots:	

There were 47 sets of responses, including comments from approximately 121 different people from approximately 93 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope 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 SAR 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
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	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
MRO	Dana Klem	1,2,3,4,5,6	MRO	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 Administration	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 Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO

					Mike Morrow	Midcontinent ISO	2	MRO
Westar Energy	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ginger Mercier	Prairie Power , Inc.	1,3	SERC
					Susan Sosbe	Wabash Valley Power Association	3	SERC
					Jennifer Brey	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		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
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Manitoba Hydro	Mike Smith	1,3,5,6		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO

Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - 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	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Jones	National Grid	3	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
					Silvia Mitchell	NextEra Energy -	6	NPCC

	Florida Power and Light Co.		
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Michael Forte	Con Ed - Consolidated Edison	1	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		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
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - 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

1. Do you agree with the proposed scope 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.

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation agrees that a cost-effective, risk-based approach for the adoption and use of cloud services is needed within industry. BES Cyber System Information could be stored on third party systems if proper controls for confidentiality, integrity, and availability are implemented for acceptable risk to the BES. For example, if BCSI is stored within a cloud server and encrypted, the entity that owns the data should be the only one with access to the encryption keys capable of decrypting the data, availability during critical emergencies, and integrity of transport layers 2 and 3.

Reclamation disagrees with the statement, “As currently drafted, the requirement is focused on access to the ‘storage location,’ and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.” The current CIP-004 standard does not exclude these methods.

Virtualization can and should be as simple as, “If it is something that needs to be protected, protect it.” Reclamation recommends registered entities be allowed to determine their risks. Reclamation is concerned that the proposed requirements will lead to increased requirements for low impact systems. The SDT must consider allocation of resources spent on managing and documenting efforts on low impact systems. The SAR seems to indicate that everyone would need specific authorization versus the current method of allowing a position of authority to delegate who may have access. More detailed categorization will require more tracking tools and create more opportunities for failure (non-compliance) without necessarily improving BES reliability or reducing risk.

Reclamation recommends the SDT focus on defining what BCSI is; specifically, if it is information carried **through** the BES Cyber System or **about** the BES Cyber System.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	No
Document Name	

Comment

The goal of restricting access to BCSI to only authorized personnel is to ensure the confidentiality, integrity, and availability of the data. Entities need to have flexibility of defining how this is accomplished. Limiting entities to specific requirements and technology hinders a company's ability to use tools that may protect them more effectively.

A good example of this problem involves access revocation requirements for BCSI. Currently we must revoke access within the next business day. Certainly, a revocation process is necessary, but a specific time frame makes it almost impossible to manage service solutions such as cloud services.

The regulatory controls that govern BCSI should guide entities to build strong risk-based data protection plans for their BCSI, not limit them to specific technologies or measures. Doing this restricts their ability to implement modern security programs and best-of-breed tools based on current and evolving threat landscapes.

While this SAR doe mention specific technologies that could assist in preventing unauthorized access to BCSI, we are concerned that it will provide only minimal expansion of what is acceptable rather than giving each entity the flexibility it needs.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	

Response

Shari Heino - Brazos Electric Power Cooperative, Inc. - 1,5

Answer	No
Document Name	

Comment

We do not believe that the standards require revision in order to accommodate cloud storage, encryption, or various other tools which may be used for protection of BCSI. CIP-004-6 is written to accommodate a variety of vetting and authorization approaches. For BSCI access under CIP-004, R4.1 merely specifies that a Responsible Entity must have a *process* to "*authorize based on need*, *as determined by the Responsible Entity*," for the types of access listed in 4.1.1 through 4.1.3. This provision does not specify a requirement to do background or identity checks on individual third party employees. It does not preclude the ability of a Responsible Entity to use a cloud provider to store BSCI; it merely requires codifying and implementing an approach to authorizing access to BCSI storage, if actual access will even occur. Terms such as "access," "designated storage location," and "termination action" are undefined in the standards, and, depending how defined in the Responsible Entity's process, could allow third party cloud storage of BSCI while still meeting the current standards.

If the drafting team determines that changes should be made; however, we recommend that, (1) such changes should be clearly couched as clarifications, and (2) highly specific or qualitative requirements regarding cloud storage and encryption should be avoided. Technology and cyber attacks are changing daily, and our requirements should remain flexible regarding the protections we choose to use.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

While Dominion Energy supports cloud computing, Dominion Energy does not support the instant SAR. In stating the industry needs to allow BCSI data to be stored on the cloud using encryption rather than the current requirements of the CIP standards, the SAR does NOT present a reliability purpose to allow this less stringent method of storage of BCSI data. The need statement actually appears to potentially create a reliability gap by asserting that encryption alone could be an alternative to the existing requirements. The SAR is proposing to use specific technologies (i.e. encryption and key

management) which could be less secure when used as an alternative to current CIP requirements.

Dominion Energy is also of the opinion that the SAR is requesting a modification solely for compliance clarification. A standard modification may not be the appropriate tool, rather Implementation Guidance should be used to clarify compliance expectation. The current requirements do not need to be modified to allow cloud storage of information and is appropriate based on the nature of the information being protected (BCSI). Dominion Energy is of the opinion that the term 'access', which is a key issue in the SAR, standard could be defined as "the ability to use" when used in the context of electronic access; therefore, a change to the standard wouldn't be necessary to allow an entity to take credit for controls that prevent access; such as, encryption and key management as methods for controlling physical/electronic access.

As an example, if an individual can log into a server that contains an electronic storage location but doesn't have the ability to use the data because the individual doesn't the rights to access the data, there's no compliance issue because the individual doesn't have the ability to use the data.

The issue statement for cloud computing is ensuring the entity has an ability to know who has access to the BCSI information. o Given the nature of the environment, it may not be clear who (outside of the entity) has access to the designated electronic storage location.

There may also be supply chain implications to be able to contractually ensure an entity is able to ensure administrators of the cloud computing vendor are not provisioned in such a way that they would ever have unauthorized access to a designated BCSI storage repository.

From a cyber-security perspective, use of cloud computing for confidential information increases the risk of information falling into the hands of a 'bad actor':

An entity loses control of the data as soon as it's in the cloud. This includes not only the storage location but the transport from the source to the third-party storage location.

Even though the BCSI may be may be encrypted, there's no assurance that a copy of the encrypted data can't be made. A copy of the encrypted data can be held by "bad actors" until such time as the technology exists to break the encryption.

It may not be clear who administratively has access to the electronic storage location from the cloud storage vendor.

The cloud storage vendor may subcontract portions of the administration of the environment.

There is no assurance that confidential files will be properly destroyed once it's determined they're no longer needed.

Due to the nature of cloud storage, multiple copies of a designated storage location may exist for redundancy in strategically placed data centers. Deleting a repository in one data center doesn't mean all copies (and backup copies) are also deleted.

For these reasons, Dominion Energy does not support this SAR and recommends that an Implementation Guidance document, which is appropriate to address the compliance concerns raised in the SAR, be explored.

Likes 1	SCANA - South Carolina Electric and Gas Co., 1,3,5,6, Shumpert RoLynda
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO

Answer	No
Document Name	

Comment

MPC agrees that CIP-004 can be updated to better accommodate cloud-based storage, however, the current scope misses out on opportunites to align

CIP-004 with the risk-based approach of CIP-012 and CIP-013. CIP-011 is currently risk based, but the examples provided in the SAR are highly prescriptive and should be considered a step backwards. The scope of this project should accommodate cloud storage by echoing CIP-012 R1 language, such as:

"The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure of BCSI. This shall be accomplished by one or more of the following means, to include BCSI that is in storage, transit, and use:

- *Encryption and key management;*
- *Physical access management;*
- *Electronic access management;*
- *Data loss prevention techniques and rights management services; or*
- *Using an equally effective method to mitigate the risk of unauthorized disclosure."*

The scope of this project needs to include authorization and access restrictions to BCSI, not to a "designated storage location".

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

Dominion Energy South Carolina (formerly SCANA) is in agreement with comments submitted by Dominion Energy (Sean Bodkin).

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Electric Reliability Council of Texas, Inc. (ERCOT) requests that the SAR expressly identify the option of creating a separate standard for solutions involving third-parties rather than embedding new requirements in existing requirements.

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Permitting methods such as encryption and key management to be utilized to as an additional protection for BCSI in transit and use allows improvements to the standard for CIP-011-2. However, cloud services are of a concern to the security of storing and allow multiple methods for controlling access to the BES Cyber System Information storage location may pose additional risks.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for	

using other efficient tools for CIP compliance activities.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

In addition to the mentioned potential modifications for CIP-004-6 R4.1.3, R4.4, R5.3 & CIP-011-2 R1, Tacoma Power recommends the SAR be extended to include review of CIP-004-6 R2.1.5 which covers training for BES Cyber System Information Handling, and CIP-011-2 R2 which deals with preventing unauthorized access to BCSI when a system is being reused or disposed.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

In general, Idaho Power Company agrees with the scope of the SAR as described. BCSI protections should be flexible enough to provide an entity with the ability to adapt to different environments and situations while still being restrictive enough to provide assurance that information is protected in storage, transit, and use.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the proposed scope of this project, and agrees that additional clarity regarding this issue is sorely needed.

Also, we would be interested to know if the drafting team has considered, or is aware if this project will impact CIP-013 specifically?

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	

Comment

Support NRECA comments.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	

Comment

Support NRECA Comments

Likes 0	
Dislikes 0	

Response

Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	Yes
Document Name	

Comment

Westar and Kansas City Power & Light are supportive of Edison Electric Institute's response to Question 1.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon agrees with the overall scope of the SAR. There are sections in the document that need clarification. Example #4.X.2, the language "may include but are not limited to…" seems to imply that entities aren't being held to any one thing specifically except identifying "… security protection(s) used to prevent unauthorized access to [BCSI] within each repository". Further define what's expectations are around "Data loss prevention techniques and rights management services" in section 4.X.2.

Example #2 4.1.3 "Physical access to physical BES Cyber System Information storage locations;" appears somewhat redundant with 4.1.4, "Physical access to unencrypted electronic BES Cyber System Information storage locations;" where this may require a fairly significant effort.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4

Answer	Yes
Document Name	

Comment
NRECA supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for using other efficient tools for CIP compliance activities.

Likes 0	
Dislikes 0	

Response

Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment
OG&E supports the comments made by EEI: Comments: EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration: *Comments are provided by SAR Section Title*: Industry Need: We recommend removing the introductory statement (i.e., “While there is no direct benefit to the reliability of the BES”), because we believe this statement conflicts with the following text, as currently written. Purpose or Goal: EEI members offer for consideration the following clarifying edits consideration: **This project is intended to** Cclarifying and **expand** the **the options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** such as encryption, etc.), **that could provide equally effective solutions for the storage, transit and access** to be utilized in the protection**ed** of BCSI **data**. Do you know of any consensus building activities in conjunction with this SAR? EEI member companies ask that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Are there alternatives that have been considered or could meet the objectives? EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits.

As a means to assist the SDT, several possible options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.**

Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy supports the project as intended; to expand available options under current Standard related to an entity to utilize changes in technologies for data storage paltforms. That said, we do believe tht further clarifiaction and development still needs to take place to define scope.

NV Energy believes the current SAR language is still too general in its statement for allowing Industry and Entities to be more flexible in performing business function and using new technologies, but NV Energy would request more clarifying language to understand the burden of accountability via evidence on the Entity to provide after this change is made. It would benefit NV Energy to know this, prior to agreeing to creation of a SDT for the project.

Keeping the subject matter only in the scope of CIP-004 and CIP-011, we agree with a SAR to address a growth for technologies.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	Yes
Document Name	

Comment
While AEP agrees with the proposed scope of the SAR, we recommend that the examples provided for possible revisions to CIP-004-6 Requirement R4 Part 4.1.3 be deleted from the SAR. The inclusion of the examples hinders the flexibility of the SDT to craft the revisons necessary to accurately address the use of encryption on BES Cyber System Information. AEP recommends the SDT work off the scope and objectives as written in the Detailed Description section of the SAR.

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
Southern Company supports the intent of the proposed SAR but believes there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. Southern Company requests that the scope of the SAR allows the SDT to specifically address and clarify the interpretation around encrypted BCSI and how encrypted data (cyphertext) does not constitute “information that can be used”, as per the BCSI definition. To consider cyphertext to still meet the definition of BCSI is in opposition to the plain language of the existing defined term, and to consider it as such nullifies any benefit to be gained or optionality for using 3rd party hosting solutions as a Registered Entity would have no control over those physically accessing the 3rd party’s data centers. Physical access to electronically stored and encrypted cyphertext should be considered outside of the scope of this SAR based on the grounds that access to cyphertext without the ability to decrypt that data should not be considered “access to BCSI.” The SAR should also clarify that the inclusion of encryption as an option to secure BCSI is in addition to other acceptable means available to Registered Entities, such as other physical and electronic security controls, and that the SAR will not force the SDT into limiting a Registered Entity’s options for complying with the Standard. Southern is concerned that the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions.

Likes 0	
Dislikes 0	

Response

Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	

Comment	
Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE suggests adding verbiage to the SAR to indicate entities should use the strongest encryption algorithm since not all encryption algorithms are secure.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Comments: The impact of nondisclosure agreements (NDAs) also should be considered on managing access to BSCI. In some cases within the NERC CIP Standards, a properly constructed NDA apparently can provide sufficient evidence of adequate information handling, and in other cases it cannot. For sensitive CIP-014 documents, for instance, an NDA is explicitly identified within the Standard (R2, R6) as sufficient for protecting the information, and in practice validating the existence of such an NDA appears to be the audit approach for the information protection aspect of CIP-014 R2 and R6. There is no effort on the part of ERO auditors to identify CIP-004 R4 and R5 details, such as who has access to the information, when they were disabled, or how or where it is stored by the third party signing the NDA. Similarly, an NDA appears audit-sufficient for BSCI or sentitive information provided to third party consultants as part of a mock audit, say, or for program improvement work, or for such information shared among regulated entities themselves as necessary for reliable operation of operation of the power grid. To date, NERC CIP auditors do not appear to require or request CIP-004-type evidence of how the third-party handled or stored the sensitive information or BCSI. The existence of the NDA is sufficient. Finally the ERO enterprise itself provides a third example of how NDAs, by themselves, are sometimes deemed sufficient for third-party handling and storage of sensitive information and BCSI. Here, the general NDA among the entity and regulator is considered sufficient, even for third-party (ERO)	

storage of sensitive information and BCSI in cloud-based systems such as webCDMS. Again, no CIP-004-type evidence is requested or expected.

In other cases, an NDA is not deemed sufficient. The most obvious case is that an NDA, by itself, does not appear to considered by NERC auditors as sufficient evidence of adequate protection of BCSI provided by an entity to a third-party cloud storage providers. In such cases, whether a proper NDA exists or not, the audit approach typically calls for review of evidence that all CIP-004 R4 and R5 requirements have been met by the third-party cloud provider.

These different audit approaches for sensitive information and BCSI under an NDA raise several questions. Under what conditions is an NDA, alone, sufficient and why? What is the expectation under CIP-004 R4 for BCSI that is protected pursuant to an NDA? Does the NDA authorize blanket access for the company to which it applies, or is individual authorization expected in addition to the NDA? If the former, what is the expectation regarding access tracking, revocations, and reviews? Including NDA issues within the SAR scope may reveal alternative paths towards secure cloud management of BCSI under NERC CIP.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG supports the proposed scope of the SAR. Proposed changes to the standards would provide industry with more tools and greater flexibility in complying with the CIP standards.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration:

***Comments are provided by SAR Section Title*:**

Industry Need: We recommend removing the introductory statement (i.e., “While there is no direct benefit to the reliability of the BES”), because we believe this statement conflicts with the following text, as currently written.

Purpose or Goal: EEI members offer for consideration the following clarifying edits consideration:

This project is intended to clarify and **expand the options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** encryption, etc.) **that could provide equally effective solutions for the storage, transit and access** to protect**ed** BCSI **data**. (*strike throughs removed due to the system not allowing its use*)

Do you know of any consensus building activities in conjunction with this SAR? EEI member companies ask that conclusions developed by the "informal team" assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Are there alternatives that have been considered or could meet the objectives? EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits.

As a means to assist the SDT, several options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.** (*strike throughs removed due to the system not allowing its use*)

Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.

Likes 0	
Dislikes 0	

Response

Darcy O'Connell - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO proposes that any third party obligations for storing BCSI in the cloud should not be embedded in the requirements but deferred to cloud vendor risk asseements

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
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	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Cassie Williams - Golden Spread Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
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	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
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	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We are in support of the scope of the SAR and believe changes to the standards will give registered entities additional options for using other methods for CIP compliance activities.	
Likes 0	
Dislikes 0	
Response	

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Darcy O'Connell - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	

The CAISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

CAISO contends that this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity's systems are unavailable.

Further, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

CAISO would also note that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should account for both.

PURPOSE OR GOAL SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply since access is prevented.

CAISO agrees that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity's obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION:

CAISO agrees with the concept of Example #1, but requests clarification on the inclusion of “virtual or non-virtual environment” on Example #1.

ADDITIONAL COMMENTS:

One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service.

Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

ERCOT offers the following additional comments for the SAR drafting team to consider.

INDUSTRY NEED SECTION

ERCOT believes this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity’s systems are unavailable.

In addition, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

ERCOT also notes that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should take both into consideration.

PURPOSE OR GOAL SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to

CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply because access is prevented.

ERCOT concurs with the SAR drafting team that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity's obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION

ERCOT agrees with the concept of Example No. 1, but requests clarification on the inclusion of "virtual or non-virtual environment" in Example No. 1.

ADDITIONAL COMMENTS

An additional area that should be considered is the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service. Finally, any new requirement language should include provisions concerning CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	
Document Name	

Comment

The NYISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

NYISO contends that the standard revision should be specific to storage of BCSI. This would include modifications to support the use of encryption as an acceptable level of protection for data being stored within third party infrastructure.

PURPOSE OR GOAL SECTION:

NYISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access.

DETAILED DESCRIPTION SECTION:

The use of encryption to ensure both integrity and confidentiality at a minimum should be the focus.

Modifications to the standards should include the establishment of acceptable levels of encryption, the management of keys, the establishment and testing of encryption for data stored and in transit to/from third party providers of cloud storage.

CIP modifications need to provide clarity in establishing what obligations the responsible entity would have in order to establish and maintain compliance and what aspects could be left to the third party provider of cloud storage.

Modifications should include noting contractural provisions that would need to be in place to assure the controls are in place (i.e. testing, alerting) and

what obligations the third party provider would have as it pertains to data destruction once contractual relationship is terminated.

ALTERNATIVES SECTION:

NYISO agrees with the concept of Example #1, but requests clarification on the inclusion of "virtual or non-virtual environment" on Example #1.

ADDITIONAL COMMENTS:

One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service.

Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Support NRECA comments.

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	
If approved, the following is provided as feedback to the NERC SDT that will be addressing the SAR: Southern Company suggests the SDT consider modifying the glossary definition of BCSI in the section of the defined term that states what is not BCSI to add language to the effect of “encrypted cyphertext without the ability to decrypt or access the encryption key”. Properly encrypted data is not actual information, but cyphertext and not useable without a “key” to decrypt it. Southern Company also suggests the SDT consider requirements for the use of two-factor authentication when accessing BCSI stored on 3rd party hosted solutions.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
NV Energy shares EEI's comments that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR. Additionally, NV Energy is unclear whether the examples provided were developed as part of the informal team that operated under the direction of the NERC Compliance Input Working Group.	
Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4

Answer	
Document Name	

Comment

NRECA appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO

Answer	
Document Name	

Comment

MPC has additional concerns regarding the ambigious term: "designated storage location". The ultimate objective of CIP-004 R4.1.3 is to protect BCSI, not a server, room, locker, computer, vehicle, etc. BCSI can be anywhere as it is stored, used, and transported. A "designated storage location" is a challenge to define and difficult to audit. A risk-based approach allows an entity to define the risk and the adequacy of the actions taken to mitigate that risk, without confining those actions to prescriptive definitions or an out-of-date or restrictive framework. The term "designated storage location" could be removed from CIP-004 altogether, with all requirements for the protection of BCSI being specified within CIP-011 in a manner similar to what is suggested above.

The examples provided in the SAR are restrictive, burdensome, and costly, and do not allow the entity to address the level of risk posed by a particular situation. MPC is strongly opposed to any language that resembles the examples provided in the SAR. The Cost Impact Assessment notes potential savings due to economies of scale. While this my be true when considering the use of cloud storage, the reality is that highly prescriptive requirements such as the examples that are provided, would significantly increase costs without an appropriate risk analysis.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

TVA supports review of the CIP-004 and CIP-011 language as currently written, specifically with regard to the use of encryption in place of physical access controls. However, TVA cautions against including discussion of specific technologies in the language of the standards that could prohibit or discourage innovation or use of emerging technologies.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	

ACES would like to thank the SAR Team for their efforts and opportunity to comment on the SAR.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Support NRECA Comments

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Support NRECA comments.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

Agree with the objective of the proposal, but are we certain that the current language of CIP-004-6 Requirement R4 Part 4.1.3 cannot accommodate third-party cloud-based encrypted BCSI? The “or” in “physical or electronic” access to designated storage locations (an undefined term that can be defined by the Responsible Entity) permits electronic authorization exclusively, relieving the Responsible Entity of any physical access concerns.

Encryption key management can be the process to authorize electronic access to BCSI. The designated storage location could be defined as the Responsible Entity's encrypted BSCI in a designated third-party data repository.

Does the requirement language need to be changed to explicitly permit, or can other options be pursued to ascertain whether or not current language can accommodate? Has anyone submitted implementation guidance for ERO endorsement showing how industry believes this can be done compliantly?

If NERC is receptive to encryption satisfying R4.1.3, a SAR may yet be required to specify minimum acceptable encryption key strength, such as NIST Advanced Encryption Standard AES 256-bit, just as minimum password length and complexity requirements are set forth in CIP-007-6 R5.5

Likes 0	
Dislikes 0	

Response

Oliver Burke - Entergy - Entergy Services, Inc. - 1

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	
Document Name	

Comment

Duke Energy would like to recommend that the drafting team consider the potential impacts of setting encryption at the document level or the repository level.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Reclamation recommends IT systems that store BCSI be certified and accredited for operation in accordance with federal and Department of Homeland Security (DHS) standards. Boundaries and security authorization(s) must be defined for systems with common security controls. National Institute of Standards and Technology (NIST) Information Management Security suggests entities should control risks by evaluating the system's or information's importance and designating the confidentiality, integrity, and availability necessary for the system or information. The entity's CIP Senior Manager or delegate should accept (approve) the risk for the responsible entity.

Additionally, the revised standards must specifically account for the requirements pertaining to Controlled Unclassified Information (CUI) in 32 CFR 2002. Reclamation recommends the SDT obtain a full understanding of overall information protection requirements, to include requirements beyond IT systems. For example, there is no mechanism to encrypt hard copy data, so physical protection requirements cannot be totally removed.

Reclamation also recommends the SDT incorporate the following definition of "Information Security" as stated in NIST SP800-12r1, *Section 1.4 Important Terminology,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf:

"Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability."

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	
Document Name	

Comment

GSOC appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR. Drafting team should consider how entities and NERC could rely on third party audit assessment of cloud services provider. They should also evaluate the requirement for access management, revocation, disposal and information protection.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP agrees with the SAR that additional considerations need to be given to other ways to protect BCSI beyond access to storage locations. There are more methods to protect BCSI and the standards need to be flexible enough to allow it. The current requirements apply to BCSI in the cloud, however, it is not feasible to expect third party providers of hosted solutions (cloud BCSI storage locations) to comply with CIP-004-06 R4.1.3 and CIP-004-6 R5.3, so entities have to look for other options – and not using cloud providers is no longer an option.

SRP suggests the SDT look for opportunities to update CIP-011 requirements to better document the types of protections in place for BCSI storage locations where the only available control is CIP-004-6 (access management), then CIP-004 applies.

SRP disagrees with an approach that encryption or masking BCSI renders it no longer BCSI. This would create a need for entities to know when information is no longer BCSI (upon encryption) and when it becomes BCSI again (upon decryption). It will be difficult to apply the current CIP-004 storage locations based requirements. SRP agrees with the SAR's approach that the standards should be updated to allow for other methods to protect BCSI. This will ensure a complete inventory of BCSI and a better overall understanding of the protections in place.

The SDT may want to consider minimum requirements (or guidance) for an approach to properly sanitize (i.e. cryptographic erase) off premise BCSI.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

Given that the Example #2 proposes a reasonable and alternative approach that permits encryption and key management to be utilized in lieu of physical/electronic access controls, we support Example #2 to be considered for modifying CIP-004-6 R4 Part 4.1.3. This encryption and key management method woud provide flexibility for entities to manage BCSI access and facilitate the cloud storage solution. Note that if the CIP-004-6 R4 Part 4.1.3 is revised using Example #2, the CIP-004-6 R4 Part 4.3 and R5 Part 5.3 should be revised in accordance with the modification of CIP-004-6 R4 Part 5.1.3.

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
The standards development team should favor non-prescriptive standards for protection of BES Cyber System Information that requires an appropriate level security within (1) individual Entities, (2) Application Providers, (3) Public Cloud Providers, (4) Entities that hold protected information for other utilities business partners, and (5) business partners that need access and temporarily retain this information.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	Project 2019-02 BES Cyber System Information Access Management
Comment Period Start Date:	3/28/2019
Comment Period End Date:	4/26/2019
Associated Ballots:	

There were 47 sets of responses, including comments from approximately 121 different people from approximately 93 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 Vice President of Engineering and Standards, Howard Gugel (via email) or at (404) 446-9693.

Questions

1. Do you agree with the proposed scope 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 SAR drafting team 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
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	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
MRO	Dana Klem	1,2,3,4,5,6	MRO	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 Administration	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 Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Westar Energy	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6			Bob Solomon	Hoosier Energy Rural	1	SERC

			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations		Electric Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ginger Mercier	Prairie Power , Inc.	1,3	SERC
					Susan Sosbe	Wabash Valley Power Association	3	SERC
					Jennifer Brey	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		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
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Lee Schuster	Duke Energy	3	FRCC

					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Manitoba Hydro	Mike Smith	1,3,5,6		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - 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	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Jones	National Grid	3	NPCC
					Sean Cavote	PSEG	4	NPCC

Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions	5	NPCC

	International Inc.		
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Michael Forte	Con Ed - Consolidated Edison	1	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC

Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		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
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - 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

1. Do you agree with the proposed scope 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.	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation agrees that a cost-effective, risk-based approach for the adoption and use of cloud services is needed within industry. BES Cyber System Information could be stored on third party systems if proper controls for confidentiality, integrity, and availability are implemented for acceptable risk to the BES. For example, if BCSI is stored within a cloud server and encrypted, the entity that owns the data should be the only one with access to the encryption keys capable of decrypting the data, availability during critical emergencies, and integrity of transport layers 2 and 3.

Reclamation disagrees with the statement, “As currently drafted, the requirement is focused on access to the ‘storage location,’ and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.” The current CIP-004 standard does not exclude these methods.

Virtualization can and should be as simple as, “If it is something that needs to be protected, protect it.” Reclamation recommends registered entities be allowed to determine their risks. Reclamation is concerned that the proposed requirements will lead to increased requirements for low impact systems. The SDT must consider allocation of resources spent on managing and documenting efforts on low impact systems. The SAR seems to indicate that everyone would need specific authorization versus the current method of allowing a position of authority to delegate who may have access. More detailed categorization will require more tracking tools and create more opportunities for failure (non-compliance) without necessarily improving BES reliability or reducing risk.

Reclamation recommends the SDT focus on defining what BCSI is; specifically, if it is information carried **through** the BES Cyber System or **about** the BES Cyber System.

Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy

Dislikes 0	
Response	
Thank you for your comment. The SAR DT has revised the SAR to more accurately state what the SDT would be addressing with the future proposed revisions. The scope of the proposed SAR is only related to High and Medium Impact BES Cyber Systems. The consideration of the definition is included in the scope of the SAR.	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	No
Document Name	
Comment	
The goal of restricting access to BCSI to only authorized personnel is to ensure the confidentiality, integrity, and availability of the data. Entities need to have flexibility of defining how this is accomplished. Limiting entities to specific requirements and technology hinders a company's ability to use tools that may protect them more effectively. A good example of this problem involves access revocation requirements for BCSI. Currently we must revoke access within the next business day. Certainly, a revocation process is necessary, but a specific time frame makes it almost impossible to manage service solutions such as cloud services. The regulatory controls that govern BCSI should guide entities to build strong risk-based data protection plans for their BCSI, not limit them to specific technologies or measures. Doing this restricts their ability to implement modern security programs and best-of-breed tools based on current and evolving threat landscapes. While this SAR doe mention specific technologies that could assist in preventing unauthorized access to BCSI, we are concerned that it will provide only minimal expansion of what is acceptable rather than giving each entity the flexibility it needs.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	

Thank you for your comment. The Requirements concerning access management and the flexibility are included in the scope of the revised SAR.	
Shari Heino - Brazos Electric Power Cooperative, Inc. - 1,5	
Answer	No
Document Name	
Comment	
We do not believe that the standards require revision in order to accommodate cloud storage, encryption, or various other tools which may be used for protection of BCSI. CIP-004-6 is written to accommodate a variety of vetting and authorization approaches. For BSCI access under CIP-004, R4.1 merely specifies that a Responsible Entity must have a *process* to "*authorize based on need, as determined by the Responsible Entity*," for the types of access listed in 4.1.1 through 4.1.3. This provision does not specify a requirement to do background or identity checks on individual third party employees. It does not preclude the ability of a Responsible Entity to use a cloud provider to store BSCI; it merely requires codifying and implementing an approach to authorizing access to BCSI storage, if actual access will even occur. Terms such as "access," "designated storage location," and "termination action" are undefined in the standards, and, depending how defined in the Responsible Entity's process, could allow third party cloud storage of BSCI while still meeting the current standards. If the drafting team determines that changes should be made; however, we recommend that, (1) such changes should be clearly couched as clarifications, and (2) highly specific or qualitative requirements regarding cloud storage and encryption should be avoided. Technology and cyber attacks are changing daily, and our requirements should remain flexible regarding the protections we choose to use.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	
Thank you for your comment. The Requirements concerning access management and the flexibility are included in the scope of the revised SAR.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No

Document Name	
Comment	

While Dominion Energy supports cloud computing, Dominion Energy does not support the instant SAR. In stating the industry needs to allow BCSI data to be stored on the cloud using encryption rather than the current requirements of the CIP standards, the SAR does NOT present a reliability purpose to allow this less stringent method of storage of BCSI data. The need statement actually appears to potentially create a reliability gap by asserting that encryption alone could be an alternative to the existing requirements. The SAR is proposing to use specific technologies (i.e. encryption and key management) which could be less secure when used as an alternative to current CIP requirements.

Dominion Energy is also of the opinion that the SAR is requesting a modification solely for compliance clarification. A standard modification may not be the appropriate tool, rather Implementation Guidance should be used to clarify compliance expectation. The current requirements do not need to be modified to allow cloud storage of information and is appropriate based on the nature of the information being protected (BCSI). Dominion Energy is of the opinion that the term 'access', which is a key issue in the SAR, standard could be defined as "the ability to use" when used in the context of electronic access; therefore, a change to the standard wouldn't be necessary to allow an entity to take credit for controls that prevent access; such as, encryption and key management as methods for controlling physical/electronic access.

As an example, if an individual can log into a server that contains an electronic storage location but doesn't have the ability to use the data because the individual doesn't the rights to access the data, there's no compliance issue because the individual doesn't have the ability to use the data.

The issue statement for cloud computing is ensuring the entity has an ability to know who has access to the BCSI information. o Given the nature of the environment, it may not be clear who (outside of the entity) has access to the designated electronic storage location.

There may also be supply chain implications to be able to contractually ensure an entity is able to ensure administrators of the cloud computing vendor are not provisioned in such a way that they would ever have unauthorized access to a designated BCSI storage repository.

From a cyber-security perspective, use of cloud computing for confidential information increases the risk of information falling into the hands of a 'bad actor':

An entity loses control of the data as soon as it's in the cloud. This includes not only the storage location but the transport from the source to the third-party storage location.

Even though the BCSI may be may be encrypted, there's no assurance that a copy of the encrypted data can't be made. A copy of the encrypted data can be held by "bad actors" until such time as the technology exists to break the encryption.

It may not be clear who administratively has access to the electronic storage location from the cloud storage vendor.

The cloud storage vendor may subcontract portions of the administration of the environment.

There is no assurance that confidential files will be properly destroyed once it's determined they're no longer needed.

Due to the nature of cloud storage, multiple copies of a designated storage location may exist for redundancy in strategically placed data centers. Deleting a repository in one data center doesn't mean all copies (and backup copies) are also deleted.

For these reasons, Dominion Energy does not support this SAR and recommends that an Implementation Guidance document, which is appropriate to address the compliance concerns raised in the SAR, be explored.

Likes 1	SCANA - South Carolina Electric and Gas Co., 1,3,5,6, Shumpert RoLynda
Dislikes 0	

Response

Thank you for your comment. The SAR DT asserts that revisions to the current standards are needed to provide further clarity.

Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO

Answer	No
Document Name	

Comment

MPC agrees that CIP-004 can be updated to better accommodate cloud-based storage, however, the current scope misses out on opportunites to align CIP-004 with the risk-based approach of CIP-012 and CIP-013. CIP-011 is currently risk based, but the examples provided in the SAR

are highly prescriptive and should be considered a step backwards. The scope of this project should accommodate cloud storage by echoing CIP-012 R1 language, such as: *"The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure of BCSI. This shall be accomplished by one or more of the following means, to include BCSI that is in storage, transit, and use:* • *Encryption and key management;* • *Physical access management;* • *Electronic access management;* • *Data loss prevention techniques and rights management services; or* • *Using an equally effective method to mitigate the risk of unauthorized disclosure."* *The scope of this project needs to include authorization and access restrictions to BCSI, not to a "designated storage location".*

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment
Dominion Energy South Carolina (formerly SCANA) is in agreement with comments submitted by Dominion Energy (Sean Bodkin).

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see response to Dominion Energy.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Electric Reliability Council of Texas, Inc. (ERCOT) requests that the SAR expressly identify the option of creating a separate standard for solutions involving third-parties rather than embedding new requirements in existing requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your participation.	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Permitting methods such as encryption and key management to be utilized to as an additional protection for BCSI in transit and use allows improvements to the standard for CIP-011-2. However, cloud services are of a concern to the security of storing and allow multiple methods for controlling access to the BES Cyber System Information storage location may pose additional risks.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for using other efficient tools for CIP compliance activities.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
In addition to the mentioned potential modifications for CIP-004-6 R4.1.3, R4.4, R5.3 & CIP-011-2 R1, Tacoma Power recommends the SAR be extended to include review of CIP-004-6 R2.1.5 which covers training for BES Cyber System Information Handling, and CIP-011-2 R2 which deals with preventing unauthorized access to BCSI when a system is being reused or disposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has revised the SAR to more accurately state what the SDT would be addressing with the future proposed revisions.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
In general, Idaho Power Company agrees with the scope of the SAR as described. BCSI protections should be flexible enough to provide an entity with the ability to adapt to different environments and situations while still being restrictive enough to provide assurance that information is protected in storage, transit, and use.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed scope of this project, and agrees that additional clarity regarding this issue is sorely needed. **Also, we would be interested to know if the drafting team has considered, or is aware if this project will impact CIP-013 specifically?**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see response to NRECA.	
Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar and Kansas City Power & Light are supportive of Edison Electric Institute's response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon agrees with the overall scope of the SAR. There are sections in the document that need clarification. Example #4.X.2, the language "may include but are not limited to…" seems to imply that entities aren't being held to any one thing specifically except identifying "… security protection(s) used to prevent unauthorized access to [BCSI] within each repository". Further define what's expectations are around "Data loss prevention techniques and rights management services" in section 4.X.2. Example #2 4.1.3 "Physical access to physical BES Cyber System Information storage locations;" appears somewhat redundant with 4.1.4, "Physical access to unencrypted electronic BES Cyber System Information storage locations;" where this may require a fairly significant effort.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	Yes
Document Name	
Comment	
NRECA supports the proposed scope of the SAR and we believe the changes to the standards will provide registered entities with additional options for using other efficient tools for CIP compliance activities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
OG&E supports the comments made by EEI: Comments: EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration:	

Comments are provided by SAR Section Title:

Industry Need: We recommend removing the introductory statement (i.e., “While there is no direct benefit to the reliability of the BES”), because we believe this statement conflicts with the following text, as currently written.

Purpose or Goal: EEI members offer for consideration the following clarifying edits consideration:

This project is intended to Cclarifying and **expand** the **options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** such as encryption, etc.), **that could provide equally effective solutions for the storage, transit and access** to be utilized in the protection**ed** of BCSI **data**.

Do you know of any consensus building activities in conjunction with this SAR? EEI member companies ask that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Are there alternatives that have been considered or could meet the objectives? EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits.

As a means to assist the SDT, several possible options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.**

Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy supports the project as intended; to expand available options under current Standard related to an entity to utilize changes in technologies for data storage paltforms. That said, we do believe tht further clarifiaction and development still needs to take place to define scope. NV Energy believes the current SAR language is still too general in its statement for allowing Industry and Entities to be more flexible in performing business function and using new technologies, but NV Energy would request more clarifying language to understand the burden of accountability via evidence on the Entity to provide after this change is made. It would benefit NV Energy to know this, prior to agreeing to creation of a SDT for the project. Keeping the subject matter only in the scope of CIP-004 and CIP-011, we agree with a SAR to address a growth for technologies.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope and we believe your concern has been addressed.	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
While AEP agrees with the proposed scope of the SAR, we recommend that the examples provided for possible revisions to CIP-004-6 Requirement R4 Part 4.1.3 be deleted from the SAR. The inclusion of the examples hinders the flexibility of the SDT to craft the revisons necessary to accurately address the use of encryption on BES Cyber System Information. AEP recommends the SDT work off the scope and objectives as written in the Detailed Description section of the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company supports the intent of the proposed SAR but believes there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System.	

Southern Company requests that the scope of the SAR allows the SDT to specifically address and clarify the interpretation around encrypted BCSI and how encrypted data (cyphertext) does not constitute "information that can be used", as per the BCSI definition. To consider cyphertext to still meet the definition of BCSI is in opposition to the plain language of the existing defined term, and to consider it as such nullifies any benefit to be gained or optionality for using 3rd party hosting solutions as a Registered Entity would have no control over those physically accessing the 3rd party's data centers. Physical access to electronically stored and encrypted cyphertext should be considered outside of the scope of this SAR based on the grounds that access to cyphertext without the ability to decrypt that data should not be considered "access to BCSI." The SAR should also clarify that the inclusion of encryption as an option to secure BCSI is in addition to other acceptable means available to Registered Entities, such as other physical and electronic security controls, and that the SAR will not force the SDT into limiting a Registered Entity's options for complying with the Standard. Southern is concerned that the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions. The SAR DT has revised the scope.	
Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Support NRECA comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE suggests adding verbiage to the SAR to indicate entities should use the strongest encryption algorithm since not all encryption algorithms are secure.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Comments: The impact of nondisclosure agreements (NDAs) also should be considered on managing access to BSCI. In some cases within the NERC CIP Standards, a properly constructed NDA apparently can provide sufficient evidence of adequate information handling, and in other cases it cannot. For sensitive CIP-014 documents, for instance, an NDA is explicitly identified within the Standard (R2, R6) as sufficient for protecting the information, and in practice validating the existence of such an NDA appears to be the audit approach for the information protection aspect	

of CIP-014 R2 and R6. There is no effort on the part of ERO auditors to identify CIP-004 R4 and R5 details, such as who has access to the information, when they were disabled, or how or where it is stored by the third party signing the NDA.

Similarly, an NDA appears audit-sufficient for BSCI or sentitive information provided to third party consultants as part of a mock audit, say, or for program improvement work, or for such information shared among regulated entities themselves as necessary for reliable operation of operation of the power grid. To date, NERC CIP auditors do not appear to require or request CIP-004-type evidence of how the third-party handled or stored the sensitive information or BCSI. The existence of the NDA is sufficient.

Finally the ERO enterprise itself provides a third example of how NDAs, by themselves, are sometimes deemed sufficient for third-party handling and storage of sensitive information and BCSI. Here, the general NDA among the entity and regulator is considered sufficient, even for third-party (ERO) storage of sensitive information and BCSI in cloud-based systems such as webCDMS. Again, no CIP-004-type evidence is requested or expected.

In other cases, an NDA is not deemed sufficient. The most obvious case is that an NDA, by itself, does not appear to considered by NERC auditors as sufficient evidence of adequate protection of BCSI provided by an entity to a third-party cloud storage providers. In such cases, whether a proper NDA exists or not, the audit approach typically calls for review of evidence that all CIP-004 R4 and R5 requirements have been met by the third-party cloud provider.

These different audit approaches for sensitive information and BCSI under an NDA raise several questions. Under what conditions is an NDA, alone, sufficient and why? What is the expectation under CIP-004 R4 for BCSI that is protected pursuant to an NDA? Does the NDA authorize blanket access for the company to which it applies, or is individual authorization expected in addition to the NDA? If the former, what is the expectation regarding access tracking, revocations, and reviews? Including NDA issues within the SAR scope may reveal alternative paths towards secure cloud management of BCSI under NERC CIP.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes

Document Name	
Comment	
PSEG supports the proposed scope of the SAR. Proposed changes to the standards would provide industry with more tools and greater flexibility in complying with the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI member companies support the intent of the proposed SAR but believe there is room to clarify the draft language to ensure the affected Reliability Standards continue to meet the Reliability needs of the Bulk Electric System. From that perspective, we offer the following brief input for consideration: ***Comments are provided by SAR Section Title*:** **Industry Need:** We recommend removing the introductory statement (i.e., "While there is no direct benefit to the reliability of the BES"), because we believe this statement conflicts with the following text, as currently written. **Purpose or Goal**: EEI members offer for consideration the following clarifying edits consideration:	

This project is intended to clarify and **expand the options available under the** CIP requirements**,** related to BES Cyber System Information access, to **remove unnecessary barriers and** allow for alternative methods, **(e.g.,** encryption, etc.) **that could provide equally effective solutions for the storage, transit and access** to protect**ed** BCSI **data**. (*strike throughs removed due to the system not allowing its use*) **Do you know of any consensus building activities in conjunction with this SAR?** EEI member companies ask that conclusions developed by the "informal team" assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR. **Are there alternatives that have been considered or could meet the objectives?** EEI member companies question whether the detailed examples contained within the SAR might unintentionally limit the SDT from developing other, possibly more effective, solutions and offer the following edits. As a means to assist the SDT, several options **are provided** for **SDT consideration to address** revision**s** to CIP-004-6 Requirement R4 Part 4.1.3. **These options are not intended to limit the SDT from developing other more effective solutions.** (*strike throughs removed due to the system not allowing its use*) Additionally, EEI member companies are unclear whether the examples provided were developed as part of the informal team (previously mentioned in the proceeding question), that operated under the direction of the NERC Compliance Input Working Group. If that is the case, we believe such information would be better placed under the proceeding question.
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to address reliability benefits and made a clarification to provided examples.	
Darcy O'Connell - California ISO - 2 - WECC	
Answer	Yes
Document Name	

Comment	
CAISO proposes that any third party obligations for storing BCSI in the cloud should not be embedded in the requirements but deferred to cloud vendor risk asseements	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT so they can request additional information for clarity.	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your participation.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Cassie Williams - Golden Spread Electric Cooperative, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your participation.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
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	
Thank you for your participation.	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
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	
Likes 0	
Dislikes 0	
Response	

Thank you for your participation.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We are in support of the scope of the SAR and believe changes to the standards will give registered entities additional options for using other methods for CIP compliance activities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

2. Provide any additional comments for the SAR drafting team to consider, if desired.	
Darcy O'Connell - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	

The CAISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

CAISO contends that this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity's systems are unavailable.

Further, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

CAISO would also note that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should account for both.

PURPOSE OR GOAL SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION:

CAISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply since access is prevented.

CAISO agrees that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity's obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION:

CAISO agrees with the concept of Example #1, but requests clarification on the inclusion of "virtual or non-virtual environment" on Example #1.

ADDITIONAL COMMENTS:

One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service.

Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

ERCOT offers the following additional comments for the SAR drafting team to consider.

INDUSTRY NEED SECTION

ERCOT believes this initiative could have a direct benefit to reliability. The use of third-party solutions (aka cloud) for the storage of BES Cyber System Information can provide a reliability benefit in having recovery plans and other information available to the entity in the event they are needed and the entity's systems are unavailable.

In addition, as technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Many of these types of software providers are no longer offering on-premises solutions. Allowing the use of third parties for these solutions to analyze and take action serves to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

ERCOT also notes that the SAR does not address the use of applications. The SAR only addresses storage. The SAR should take both into consideration.

PURPOSE OR GOAL SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1.

DETAILED DESCRIPTION SECTION

Encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent "unauthorized retrieval" of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access. The use of encryption should be applied consistently to CIP-004 R4, CIP-004 R5, and CIP-011 R2, Part 2.1. The use of encryption can be used to prevent access. Therefore, CIP-004 R4 and R5 should not apply because access is prevented.

ERCOT concurs with the SAR drafting team that audit evidence should be addressed. This should include the use of external audit reports to demonstrate compliance in lieu of detailed evidence that would be available for on-premises implementations. In the context of these services, the Responsible Entity’s obligations may only be limited to due diligence in reviewing third party audit and certification details.

ALTERNATIVES SECTION

ERCOT agrees with the concept of Example No. 1, but requests clarification on the inclusion of "virtual or non-virtual environment" in Example No. 1.

ADDITIONAL COMMENTS

An additional area that should be considered is the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service. Finally, any new requirement language should include provisions concerning CIP Exceptional Circumstance in addressing access controls under CIP-004.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	
Document Name	
Comment	

The NYISO offers the following feedback on the SAR.

INDUSTRY NEED SECTION:

NYISO contends that the standard revision should be specific to storage of BCSI. This would include modifications to support the use of encryption as an acceptable level of protection for data being stored within third party infrastructure.

PURPOSE OR GOAL SECTION:

NYISO contends that encryption is already recognized as a means to protect BCSI. Under CIP-011-2 R2, Part 2.1, encryption is listed as a means to prevent “unauthorized retrieval” of BCSI. Unauthorized retrieval is basically the same concept as unauthorized access.

DETAILED DESCRIPTION SECTION:

The use of encryption to ensure both integrity and confidentiality at a minimum should be the focus.

Modifications to the standards should include the establishment of acceptable levels of encryption, the management of keys, the establishment and testing of encryption for data stored and in transit to/from third party providers of cloud storage.

CIP modifications need to provide clarity in establishing what obligations the responsible entity would have in order to establish and maintain compliance and what aspects could be left to the third party provider of cloud storage.

Modifications should include noting contractural provisions that would need to be in place to assure the controls are in place (i.e. testing, alerting) and what obligations the third party provider would have as it pertains to data destruction once contractual relationship is terminated. **ALTERNATIVES SECTION:** NYISO agrees with the concept of Example #1, but requests clarification on the inclusion of "virtual or non-virtual environment" on Example #1. **ADDITIONAL COMMENTS:** One area that should be considered is to address the geographical location of BCSI stored with a third party (aka cloud). Requirements should be drafted for entities to evaluate the geographic location of hosted solutions in their risk assessment of the service. Any requirement language should include provisions of a CIP Exceptional Circumstance in addressing access controls under CIP-004.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility and geographical location. This will be noted for the SDT to consider as they draft proposed revisions.	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Thank you for your participation.	
Jerry Horner - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	
Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
If approved, the following is provided as feedback to the NERC SDT that will be addressing the SAR:	

Southern Company suggests the SDT consider modifying the glossary definition of BCSI in the section of the defined term that states what is not BCSI to add language to the effect of “encrypted cyphertext without the ability to decrypt or access the encryption key”. Properly encrypted data is not actual information, but cyphertext and not useable without a “key” to decrypt it.

Southern Company also suggests the SDT consider requirements for the use of two-factor authentication when accessing BCSI stored on 3rd party hosted solutions.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	

Comment
NV Energy shares EEI's comments that conclusions developed by the “informal team” assembled by the NERC Compliance Input Working Group be referenced within this SAR. While it is clear that a large number of SMEs worked on this effort, their findings and recommendations are neither posted by NERC or referenced within this SAR.

Additionally, NV Energy is unclear whether the examples provided were developed as part of the informal team that operated under the direction of the NERC Compliance Input Working Group.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	
Document Name	
Comment	
NRECA appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Andy Fuhrman - Minnkota Power Cooperative Inc. - NA - Not Applicable - MRO	
Answer	
Document Name	
Comment	
MPC has additional concerns regarding the ambigious term: "designated storage location". The ultimate objective of CIP-004 R4.1.3 is to protect BCSI, not a server, room, locker, computer, vehicle, etc. BCSI can be anywhere as it is stored, used, and transported. A "designated storage location" is a challenge to define and difficult to audit. A risk-based approach allows an entity to define the risk and the adequacy of	

the actions taken to mitigate that risk, without confining those actions to prescriptive definitions or an out-of-date or restrictive framework. The term "designated storage location" could be removed from CIP-004 altogether, with all requirements for the protection of BCSI being specified within CIP-011 in a manner similar to what is suggested above. *The examples provided in the SAR are restrictive, burdensome, and costly, and do not allow the entity to address the level of risk posed by a particular situation. MPC is strongly opposed to any language that resembles the examples provided in the SAR. The Cost Impact Assessment notes potential savings due to economies of scale. While this my be true when considering the use of cloud storage, the reality is that highly prescriptive requirements such as the examples that are provided, would significantly increase costs without an appropriate risk analysis.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has addressed the concerns with revisions to the SAR concerning "designated storage location." This will be noted for the SDT to consider as they draft proposed revisions.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
TVA supports review of the CIP-004 and CIP-011 language as currently written, specifically with regard to the use of encryption in place of physical access controls. However, TVA cautions against including discussion of specific technologies in the language of the standards that could prohibit or discourage innovation or use of emerging technologies.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The SAR DT agrees that it should be about the “what” and not the “how”. This will be noted for the SDT to consider as they draft proposed revisions.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Douglas Webb - Westar Energy - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	
Document Name	
Comment	
ACES would like to thank the SAR Team for their efforts and opportunity to comment on the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jeremy Voll - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	
Support NRECA Comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	

Support NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to NRECA.	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
Agree with the objective of the proposal, but are we certain that the current language of CIP-004-6 Requirement R4 Part 4.1.3 cannot accommodate third-party cloud-based encrypted BCSI? The “or” in “physical or electronic” access to designated storage locations (an undefined term that can be defined by the Responsible Entity) permits electronic authorization exclusively, relieving the Responsible Entity of any physical access concerns. Encryption key management can be the process to authorize electronic access to BCSI. The designated storage location could be defined as the Responsible Entity’s encrypted BSCI in a designated third-party data repository. Does the requirement language need to be changed to explicitly permit, or can other options be pursued to ascertain whether or not current language can accommodate? Has anyone submitted implementation guidance for ERO endorsement showing how industry believes this can be done compliantly? If NERC is receptive to encryption satisfying R4.1.3, a SAR may yet be required to specify minimum acceptable encryption key strength, such as NIST Advanced Encryption Standard AES 256-bit, just as minimum password length and complexity requirements are set forth in CIP-007-6 R5.5	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SAR DT asserts that revisions to the current standards are needed to provide further clarity.	
Oliver Burke - Entergy - Entergy Services, Inc. - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy would like to recommend that the drafting team consider the potential impacts of setting encryption at the document level or the repository level.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation recommends IT systems that store BCSI be certified and accredited for operation in accordance with federal and Department of Homeland Security (DHS) standards. Boundaries and security authorization(s) must be defined for systems with common security controls. National Institute of Standards and Technology (NIST) Information Management Security suggests entities should control risks by evaluating the system's or information's importance and designating the confidentiality, integrity, and availability necessary for the system or information. The entity's CIP Senior Manager or delegate should accept (approve) the risk for the responsible entity.

Additionally, the revised standards must specifically account for the requirements pertaining to Controlled Unclassified Information (CUI) in 32 CFR 2002. Reclamation recommends the SDT obtain a full understanding of overall information protection requirements, to include requirements beyond IT systems. For example, there is no mechanism to encrypt hard copy data, so physical protection requirements cannot be totally removed.

Reclamation also recommends the SDT incorporate the following definition of "Information Security" as stated in NIST SP800-12r1, *Section 1.4 Important Terminology,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf:

"Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability."

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	

Document Name	
Comment	
GSOC appreciates the efforts of Tri-State G&T and the other members of the NERC Compliance Input Working Group for submitting this SAR. Drafting team should consider how entities and NERC could rely on third party audit assessment of cloud services provider. They should also evaluate the requirement for access management, revocation, disposal and information protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SAR that additional considerations need to be given to other ways to protect BCSI beyond access to storage locations. There are more methods to protect BCSI and the standards need to be flexible enough to allow it. The current requirements apply to BCSI in the cloud, however, it is not feasible to expect third party providers of hosted solutions (cloud BCSI storage locations) to comply with CIP-004-06 R4.1.3 and CIP-004-6 R5.3, so entities have to look for other options – and not using cloud providers is no longer an option. SRP suggests the SDT look for opportunities to update CIP-011 requirements to better document the types of protections in place for BCSI storage locations where the only available control is CIP-004-6 (access management), then CIP-004 applies. SRP disagrees with an approach that encryption or masking BCSI renders it no longer BCSI. This would create a need for entities to know when information is no longer BCSI (upon encryption) and when it becomes BCSI again (upon decryption). It will be difficult to apply the	

current CIP-004 storage locations based requirements. SRP agrees with the SAR's approach that the standards should be updated to allow for other methods to protect BCSI. This will ensure a complete inventory of BCSI and a better overall understanding of the protections in place. The SDT may want to consider minimum requirements (or guidance) for an approach to properly sanitize (i.e. cryptographic erase) off premise BCSI.	
Likes 1	Minnkota Power Cooperative Inc., NA - Not Applicable, Fuhrman Andy
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	
Document Name	
Comment	

Given that the Example #2 proposes a reasonable and alternative approach that permits encryption and key management to be utilized in lieu of physical/electronic access controls, we support Example #2 to be considered for modifying CIP-004-6 R4 Part 4.1.3. This encryption and key management method woud provide flexibility for entities to manage BCSI access and facilitate the cloud storage solution. Note that if the CIP-004-6 R4 Part 4.1.3 is revised using Example #2, the CIP-004-6 R4 Part 4.3 and R5 Part 5.3 should be revised in accordance with the modification of CIP-004-6 R4 Part 5.1.3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This will be noted for the SDT to consider as they draft proposed revisions.	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
The standards development team should favor non-prescriptive standards for protection of BES Cyber System Information that requires an appropriate level security within (1) individual Entities, (2) Application Providers, (3) Public Cloud Providers, (4) Entities that hold protected information for other utilities business partners, and (5) business partners that need access and temporarily retain this information.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SAR DT has made revisions to the scope as well as addressing the flexibility. The SDT should consider issues related to where data resides (e.g. off premises). This will be noted for the SDT to consider as they draft proposed revisions.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2019-02 BES Cyber System Information Access Management** SAR drafting team members by **8 p.m. Eastern, Friday, April 26, 2019.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

BES Cyber System Information Access Management
The purpose of this project is to clarify the CIP requirements related to BES Cyber System Information (BCSI) access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI.

Standard affected: CIP-004-6 and CIP-011-2
The Reliability Standard(s) developed or revised will include modifications to clarify authorization and access to the BCSI to focus on the BCSI and the controls deployed to limit access. In addition, revisions should allow multiple methods for controlling access to BES Cyber System Information, rather than just electronic and physical access to the BES Cyber System Information storage location. For example, the focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (aka cloud). As currently drafted, the requirement is focused on access to the "storage location," and therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.

The time commitment for these projects is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

We are seeking a cross section of the industry to participate on the team, but in particular are seeking individuals who have experience and expertise in one or more of the following areas:

- BES Cyber System Information (BCSI) access management
- Critical Infrastructure Protection ("CIP") family of Reliability Standards

Individuals who have facilitation skills and experience and/or legal or technical writing backgrounds are also strongly desired. Please include this in the description of qualifications as applicable.

Name:	
Organization:	
Address:	
Telephone:	
Email:	
Please briefly describe your experience and qualifications to serve on the requested standard drafting team (Bio):	
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	☐ WECC
☐ FRCC	☐ RF	☐ NA – Not Applicable
☐ MRO	☐ SERC	

Select each Industry Segment that you represent:

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

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

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

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

Organization:		Email:	

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 2019-02 BES Cyber System Information Access Management

Nomination Period Open through April 26, 2019

Now Available

Nominations are being sought for SAR drafting team members through **8 p.m. Eastern, Friday, April 26, 2019**.

Use the electronic form to submit a nomination. If you experience issues using the electronic form, contact Linda Jenkins. An unofficial Word version of the nomination form is posted on the Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be two face-to-face meetings per quarter (on average three full working days each meeting) with conference calls scheduled as needed to meet the agreed upon timeline the team sets forth. Team members may also have side projects, either individually or by sub-group, to present for discussion and review. Lastly, an important component of the team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful ballot.

Previous drafting or periodic review team experience is beneficial, but not required. See the project page and unofficial nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the team May 22, 2019. Nominees will be notified shortly after they have been selected**.**

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

For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g., cloud services).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information.			
Project Scope (Define the parameters of the proposed project):			
The scope of this project is to consider CIP-004 and CIP-011 modifications, and review the NERC Glossary of Terms as it pertains to Requirements addressing BCSI.			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should not consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
SAR Drafting Team asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system (aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

Name	**Company**

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC Observer
Lonnie Ratliff	NERC Observer
Brian Kinstad	MRO Observer
Holly Eddy	WECC Observer
Kenath Carver	Texas Reliability Entity, Inc. Observer
Michael Taube	MRO Observer
Mike Stuetzle	NPCC Observer
Morgan King	WECC Observer
Shon Austin	Reliability First Observer
Tremayne Brown	SERC Observer

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. These examples are not intended to limit the SDT from developing other more effective solutions.

Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

Requested information

As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below:

EXAMPLE #1:
[Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:]
R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include:
4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.;
4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following:

- Encryption and key management,
- Physical access management,
- Electronic access management,
- Data loss prevention techniques and rights management services.

4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances;

EXAMPLE #2:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;
4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and
4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

EXAMPLE #3:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Access to electronic BES Cyber System Information.

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

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
~~While there is no direct benefit to the reliability of the BES, t~~This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utili~~t~~zation of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g.,~~aka~~ cloud services).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements and measures related to both managing access~~ing~~ and securing BES Cyber System Information~~ access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI~~.			
Project Scope (Define the parameters of the proposed project):			
The scope of this project is to consider ~~revisions modifications of~~ CIP-004 and CIP-011 modifications, and review the NERC Glossary of Terms as it pertains to Requirements addressing BCSI.			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirements ~~R4 Part 4.1.3~~ needs ~~to~~ be modified so ~~authorization~~ management of ~~and~~ access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow ~~multiple~~ various methods for controlling access to BES Cyber System Information, ~~rather than just electronic and physical access to the BES Cyber System Information~~ storage location(s). ~~For example, t~~The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g.~~aka~~ cloud services). ~~As currently drafted, t~~The current ~~r~~Requirements ~~is~~are focused on access to the "storage location", ~~and~~ but should not consider management of access to BCSI while in transit, storage, and in use. ~~therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.~~ In addition to ~~modifying~~ CIP-004-6 modifications, ~~Requirement R4 Part 4.1.3, Part 4.4, Part 5.3 and~~ CIP-011-2 ~~Requirement R1~~ should also be evaluated for any subsequent impacts ~~to the requirements, measures and/or the guidelines and technical basis~~.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
SAR Drafting Team asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any ~~i~~consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

(aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

Name	Company
Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC Observer
Lonnie Ratliff	NERC Observer
Brian Kinstad	MRO Observer
Holly Eddy	WECC Observer
Kenath Carver	Texas Reliability Entity, Inc. Observer
Michael Taube	MRO Observer
Mike Stuetzle	NPCC Observer
Morgan King	WECC Observer
Shon Austin	Reliability First Observer
Tremayne Brown	SERC Observer

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. These examples are not intended to limit the SDT from developing other more effective solutions.

Requested information

Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below:

EXAMPLE #1:
[Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:]
R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include:
4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.;
4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following:

- Encryption and key management,
- Physical access management,
- Electronic access management,
- Data loss prevention techniques and rights management services.

4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances;

EXAMPLE #2:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;
4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and
4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

EXAMPLE #3:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;

Requested information
4.1.3. Physical access to physical BES Cyber System Information storage locations; 4.1.4. Access to electronic BES Cyber System Information.

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

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting nominations. Use the electronic form to submit nominations by **8 p.m. Eastern, September 20, 2019.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information about this project is available on the Project 2019-02 BES Cyber System Information Access Management project page. If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

BES Cyber System Information Access Management
The purpose of this project is to clarify the CIP requirements and measures related to both managing access and securing BES Cyber System Information (BCSI).

Standards affected: CIP-004-6 and CIP-011-2
The Reliability Standard(s) developed or revised will include modifications so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard(s) should allow various methods for controlling access to BCSI, storage location(s). The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location," but should not consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

The time commitment for these projects is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

We are seeking a cross section of the industry to participate on the team, but in particular are seeking individuals who have experience and expertise in one or more of the following areas:

- BES Cyber System Information (BCSI) access management
- Critical Infrastructure Protection ("CIP") family of Reliability Standards

Individuals who have facilitation skills and experience and/or legal or technical writing backgrounds are also strongly desired. Please include this in the description of qualifications as applicable.

Name:	
Organization:	
Address:	
Telephone:	
Email:	
Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):	
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:		
☐ MRO ☐ NPCC	☐ RF ☐ SERC	☐ Texas RE ☐ WECC ☐ 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	

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

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	
Name:		Telephone:	
Organization:		Email:	
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 2019-02 BES Cyber System Information Access Management

Standard Drafting Team Nomination Period Open through September 20, 2019

Now Available

Additional nominations are being sought for standard drafting team (SDT) members through **8 p.m. Eastern, Friday, September 20, 2019**. This nomination period is needed to supplement the SDT.

Use the electronic form to submit a nomination. Contact Linda Jenkins regarding issues using the electronic form. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed upon timeline the team sets forth. Team members may also have side projects, either individually or by sub-group, to present for discussion and review. Lastly, an important component of the SDT effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful ballot.

Previous SDT experience is beneficial but not required. See the project page and nomination form for additional information.

Next Steps

The Standards Committee is expected to appoint members to the SDT on October 23, 2019. Nominees will be notified shortly after they have been appointed.

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

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2019-02 BES Cyber System Information Access Management” in the Description Box. For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g., cloud services).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information.			
Project Scope (Define the parameters of the proposed project):			
The scope of this project is to consider CIP-004 and CIP-011 modifications, and review the NERC Glossary of Terms as it pertains to Requirements addressing BCSI.			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
SAR Drafting Team asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system (aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

Name	**Company**

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC Observer
Lonnie Ratliff	NERC Observer
Brian Kinstad	MRO Observer
Holly Eddy	WECC Observer
Kenath Carver	Texas Reliability Entity, Inc. Observer
Michael Taube	MRO Observer
Mike Stuetzle	NPCC Observer
Morgan King	WECC Observer
Shon Austin	Reliability First Observer
Tremayne Brown	SERC Observer

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. These examples are not intended to limit the SDT from developing other more effective solutions.

Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

Requested information

As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below:

EXAMPLE #1:
[Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:]
R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include:
4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.
4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following:

- Encryption and key management,
- Physical access management,
- Electronic access management,
- Data loss prevention techniques and rights management services.

4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances;

EXAMPLE #2:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;
4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and
4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

EXAMPLE #3:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Access to electronic BES Cyber System Information.

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

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g., cloud services).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information.			
Project Scope (Define the parameters of the proposed project):			
The scope of this project is to consider CIP-004 and CIP-011 modifications, and review the NERC Glossary of Terms as it pertains to Requirements addressing BCSI.			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should ~~not~~ consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
SAR Drafting Team asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system (aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

Name	**Company**

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC Observer
Lonnie Ratliff	NERC Observer
Brian Kinstad	MRO Observer
Holly Eddy	WECC Observer
Kenath Carver	Texas Reliability Entity, Inc. Observer
Michael Taube	MRO Observer
Mike Stuetzle	NPCC Observer
Morgan King	WECC Observer
Shon Austin	Reliability First Observer
Tremayne Brown	SERC Observer

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. These examples are not intended to limit the SDT from developing other more effective solutions.

Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

Requested information
As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below: EXAMPLE #1: [Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:] R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include: 4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.; 4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following: • Encryption and key management, • Physical access management, • Electronic access management, • Data loss prevention techniques and rights management services. 4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances; EXAMPLE #2: R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; 4.1.3. Physical access to physical BES Cyber System Information storage locations; 4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations; 4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and 4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information. EXAMPLE #3: R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; 4.1.3. Physical access to physical BES Cyber System Information storage locations; 4.1.4. Access to electronic BES Cyber System Information.

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

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

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.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-7

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

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

4.1.2.2. Each 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. 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:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

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-004-7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 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.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, emails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access into a Physical Security Perimeter.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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 Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic accessor unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.4)			

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

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.

A. Introduction

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

2. **Number:** CIP-004-~~6~~7

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~Special Protection System (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.**~~**4.1.5. Reliability Coordinator**

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~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 ~~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-004-~~6~~7:

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-004-~~6~~7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 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.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~6~~7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~6~~7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and~~,~~ unescorted physical access into a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

~~CIP-004-7 Table R4 – Access Management Program~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS; and~~ ~~3. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~2. EACMS; and~~ ~~2. PACS~~	~~Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.~~	~~An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:~~ ~~1. A dated listing of authorizations for BES Cyber System information;~~ ~~2. Any privileges associated with the authorizations; and~~ ~~3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions~~

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

~~CIP-004-6~~7 Table R5 – Access Revocation			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~0. EACMS; and~~ ~~0. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~0. EACMS; and~~ ~~0. PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.~~	~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.~~

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 5.1~~ or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~5~~4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access~~,~~or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were~~	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were~~	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage~~	~~incorrect or unnecessary. (4.4)~~	~~incorrect or unnecessary. (4.4)~~	incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~locations, privileges were incorrect or unnecessary. (4.4)~~			
R5	**Same Day Operations and Operations Planning**	**Medium**	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or~~,~~ unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of the termination action. (5.3)~~ ~~OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4~~3~~) OR The Responsible	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the~~	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective~~	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.~~5~~4) OR The Responsible	~~termination action. (5.3)~~	~~date and time of the termination action. (5.3)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.~~5~~4)			

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES

Version	Date	Action	Change Tracking
			Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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:~~

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

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

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

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

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

~~Requirement R2:~~

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven-year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing~~

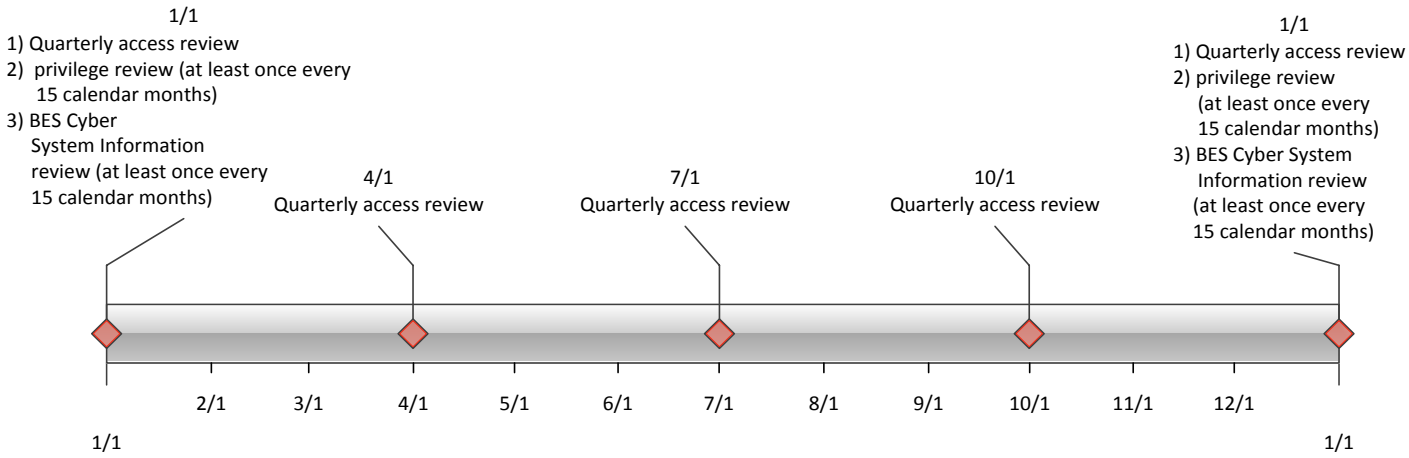
~~collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under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

~~**Requirement R4:**~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

~~**Rationale:**~~

~~During 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:**~~

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

~~**Rationale for Requirement R2:**~~

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

~~**Rationale for Requirement R3:**~~

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

~~**Rationale for Requirement R4:**~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~**hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.**~~

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

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

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.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against 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 or 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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-011-3.

6. Background:

Standard CIP-011 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicability Systems" column further defines 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-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	System information pertaining to: 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	Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Storage locations identified for housing BES Cyber System Information in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information and key management program, retention in the Physical Security Perimeter).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal			
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	Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

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 Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key management program. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (3.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (3.1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R3)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019

Anticipated Actions	Date
45-day formal or informal comment period with ballot	December 2019
45-day formal or informal comment period with additional ballot	February 2020
10-day final ballot	April 2020
Board adoption	May 2020

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.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~2~~3

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-~~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. Effective Dates:

See Implementation Plan for CIP-011-~~2~~3.

6. Background:

Standard CIP-011 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicability Systems" column ~~to~~ further defines 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-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.1	System information pertaining to: High ~~-~~Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; ~~and~~ 2. PACS; and ~~2.~~3. PCA	~~Method~~Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Examples of acceptable evidence include, but are not limited to, the following: • Documented ~~method~~ process(es) to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • ~~Repository or electronic and physical~~ Storage locations identified ~~designated~~ for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.2	BES Cyber System Information as identified in Requirement R1 Part 1.1. ~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~PACS~~	~~Procedure~~Method(s) to prevent unauthorized access to ~~for protecting and securely handling~~ BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during~~, including~~ storage, transit, use, and disposal~~-~~.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to prevent the unauthorized access to ~~Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of~~ BES Cyber System Information (e.g., encryption of ~~; or~~ • ~~Records indicating that~~ BES Cyber System Information and key management program, retention in the Physical Security Perimeter)~~is handled in a manner consistent with the entity's documented procedure(s)~~.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.4	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of acceptable evidence may include, but are not limited to, dated documentation of all of the following: • Methodology(ies) used to perform risk assessments • Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity; • Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months; • Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and • Dated documentation of action plans and statuses of remediation and/or mitigation action items.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. [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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R3~~2~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M~~2~~3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~3~~2.1	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	Prior to the release for reuse or disposal of applicable Cyber Assets ~~that contain BES Cyber System Information~~ (except for reuse within other systems identified in the "Applicable Systems" column), ~~the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from~~ the Cyber Asset data storage media shall be sanitized or destroyed.	Examples of acceptable evidence include, but are not limited to, the following: • ~~Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or~~ • ~~Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.~~ Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal. • Records that indicate chain of custody was implemented.

~~CIP-011-2 Table R2 — BES Cyber Asset Reuse and Disposal~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~2.2~~	~~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~~	~~Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence include, but are not limited to:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

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-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)~~N/A~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**~~Lower~~Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented processes for BES Cyber System Information key

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						management program. (R2)
R~~2~~3	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (~~2~~3.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (~~2~~3.~~2~~1)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~3 Table R~~2~~3 – BES Cyber Asset Reuse and Disposal. (R~~2~~3)

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 information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BES Cyber System Information.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.)~~

~~can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for

quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3.

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Establish and/or modify vendor relationships to establish compliance with the revised CIP-011-3 Requirements;
- Address the increased scope of the CIP-011-3 "Applicable Systems" and "Applicability" column, which has a focus on BES Cyber System Information as well as the addition of Protected Cyber Assets (PCA); and
- Develop additional sanitization programs for the life cycle of BES Cyber Systems, if necessary.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

CIP-004-7 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-3 – Cyber Security - Information Protection
Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-02 BES Cyber System Information Access Management** by **8 p.m. Eastern, February 3, 2020.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

Background Information

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Questions

1. The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

   ☐ Yes
   ☐ No

   Comments:

2. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

   ☐ Yes
   ☐ No

   Comments:

3. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

   ☐ Yes
   ☐ No

   Comments:

4. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

   ☐ Yes
   ☐ No

   Comments:

5. The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

   ☐ Yes
   ☐ No

   Comments:

6. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

   ☐ Yes
   ☐ No

   Comments:

7. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

   ☐ Yes
   ☐ No

   Comments:

8. The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

   ☐ Yes
   ☐ No

   Comments:

9. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

   ☐ Yes
   ☐ No

   Comments:

10. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

    ☐ Yes
    ☐ No

    Comments:

11. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

    ☐ Yes
    ☐ No

    Comments:

12. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

    ☐ Yes
    ☐ No

    Comments:

13. Do you have any other general recommendations/considerations for the drafting team?

☐ Yes
☐ No

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-004-7

December 2019

CIP-004-7 – Personnel & Training

Rationale for Requirement R4

The standard drafting team (SDT) utilized the concept of separating the association of BES Cyber System Information (BCSI) and the BES Cyber System with associated applicable systems within the CIP-004 Standard. This approach was decided to allow for maturity in the CIP-011 Information Protection Standard, facilitate future iterations of CIP-004, and remove confusion regarding protection of BCSI and BES Cyber System with associated applicable systems due to the Applicable Systems column in the requirement.

CIP-011 will include the complete lifecycle of information related to BCSI (i.e., identification, protection, access management, and disposal), thus focusing on protection and access management on BCSI itself, as appropriate. The diverse needs of entities can be addressed directly without causing confusion or affecting access management of BCSI and associated repositories. This will allow future standard development for information protection to mature in an easier fashion without disturbing requirements that involve access management of BES Cyber Systems and their associated applicable systems that may require electronic and /or physical security perimeters.

Physical access to BCSI can now be addressed separately from access to specific host media / devices whether a designated storage location or a BES Cyber System and its associated applicable systems.

This will allow the SDT the ability to move away from specifically having requirements around putting controls pertaining to designated storage locations or BES Cyber Systems and their associated applicable systems. The focus will move to implementing controls to address BCSI regardless of where the media resides at any given time.

Rationale for Requirement R4, Part 4.1.3

The intent of Requirement R4, Part 4.1.3, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, the language was removed from Requirement R4, Part 4.1.

Rationale for Deletion of Requirement R4, Part 4.4

The intent of Requirement R4, Part 4.4, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, this requirement is being recommended for retirement.

Rationale for Deletion of Requirement R5, Part 5.3

The intent of Requirement R5, Part 5.3, is now addressed in the revised version of CIP-011 regarding BCSI access management; therefore, this requirement is being recommended for retirement.

Rationale for Deletion of Requirement R5, Part 5.4

The language connecting this requirement to Requirement R5, Part 5.3, has been removed since the SDT is recommending the retirement of Requirement R5, Part 5.3.

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-004-6 standard to preserve any historical references.

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

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

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:
Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals

needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

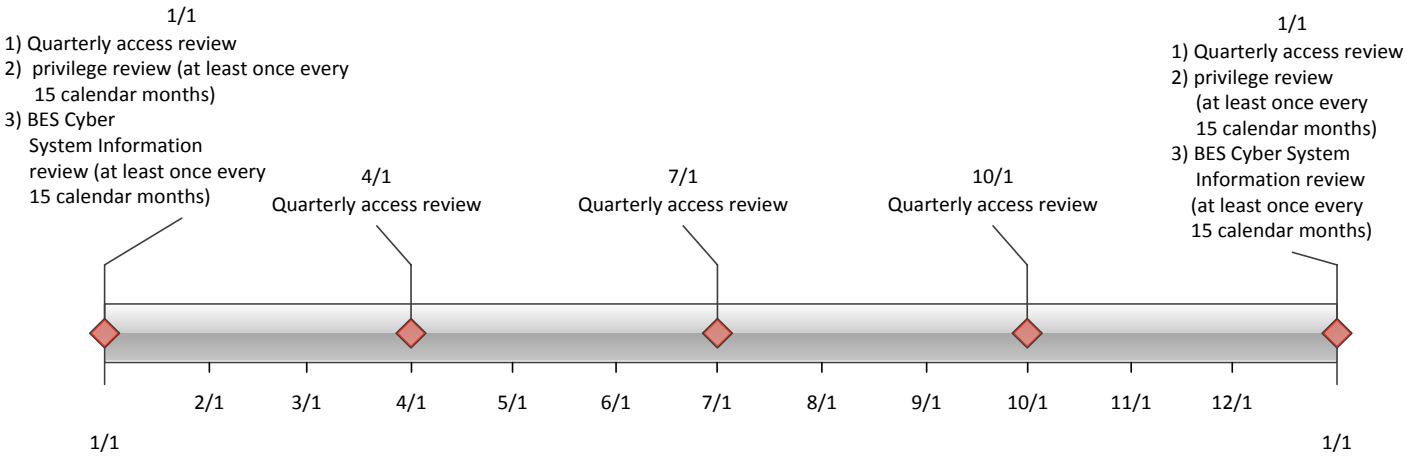
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal

history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:
Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

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

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

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

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

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

Requirement R5:
The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.

Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

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

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

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

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

Requirement 5.5 specified that passwords for shared accounts are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may

require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

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

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

Rationale for Requirement R5:
The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-011-3

December 2019

CIP-011-3 – Information Protection

Rationale for Applicability Section
Standard CIP-011 has been modified to enhance protection of BES Cyber System Information (BCSI). The modified requirements under CIP-011 will address protection of information in several facets that are discussed in this document, which include the following:

- Identification of BCSI
- Prevention of unauthorized access to BCSI
- Authorization of approved access to BCSI
- Risk assessments for BCSI not stored in the Responsible Entity's environment
- Termination of access to BCSI
- Review of access BCSI
- Key management to restrict access to BCSI
- Controls to separate duties for protecting BCSI

To provide clarity, the Applicability Systems column, which now contains BCSI, was included to associate the requirement and address the focus on protecting the BCSI regardless of the location of the BCSI. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

To address access-management-related requirements for BCSI, the related requirements from CIP-004-6 (Requirement R4, Parts 4.1.3 and 4.4, and Requirement R5, Part 5.3) have been transferred to CIP-011. This allows CIP-011 to become a more mature and easier standard to follow and update for future modifications.

Rationale for Modifications to Requirement R1, Part 1.1
Requirement R1, Part 1.1, is intended to solely identify BCSI and provide documented methods to support this identification process.

The standard drafting team (SDT) clarified the intent of addressing BCSI as opposed to the BES Cyber System (BCS) with associated applicable systems, which may contain BCSI; the Applicable Systems column

has added language to specify system information that is affiliated with High Impact and Medium Impact BES Cyber Systems and their associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Protected Cyber Assets were added to the Applicability column to ensure system information pertaining to Protected Cyber Assets is reviewed within the Responsibility Entity's information protection program subject to CIP-011 requirements, which was not previously required. Protected Cyber Assets are also applicable to CIP-011-3, Requirement R1, Parts 1.2 through 1.6, and CIP-011-3, Requirement R2, Parts 2.1 and 2.2.

Requirement language was added to Requirement R1, Part 1.1, to identify designated BCSI storage locations, whether physical or electronic. This identification should be as follows:

1) Defined as a friendly name of the electronic or physical repository (thus protecting the actual storage location); and
2) The description of the storage location (e.g., physical or electronic, off-premises or on premises).

The SDT wanted to ensure access management controls were focused on access to BCSI rather than access to BCSI designated storage locations. If a BCSI designated storage location was not identified because it does not exist, this would provide a means of accounting and clarifying this potential scenario.

The SDT has intentionally not included Low Impact BCS and their associated systems in CIP-011. Requirement R1, Part 1.1, only includes High Impact and Medium Impact BCS and their associated systems (PACS, EACMS, and PCA). The SDT also referenced Requirement R1, Part 1.1, in the Applicability column of Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Parts 2.1 and 2.2, so the Responsible Entity can easily determine the applicability of those sub-requirements based on how the Responsible Entity defined and identified BCSI to satisfy Requirement R1, Part 1.1. This further clarifies there is no CIP-011 applicability to Low Impact BCS and their associated systems.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, addresses protecting and securely handling BCSI throughout its life cycle. This life cycle includes creation, use, exchange or sharing (i.e., transit), storage, and disposal. A key component of the information protection of BCSI is the secure handling of BCSI during each of these life cycle phases.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Language was added to incorporate the NERC CMEP Practice Guide where BCSI access is defined as the ability to obtain and use BCSI.

Requirement language was revised to reflect consistency with other CIP requirements as well as the current rationale for CIP-011-2, Requirement R1 (e.g., prevent unauthorized access).

Requirement language was added to include disposal as part of the BCSI life cycle. While it is assumed that disposal of BCSI is part of the BCSI life cycle, it was not previously required.

Rationale for New Requirement R1, Part 1.3
New Requirement R1, Part 1.3, was transferred from CIP-004-6, Requirement R4, Part 4.1.3, to consolidate into one Standard both BCSI protection and access authorization to BCSI.

The SDT wanted to separate the concept of protecting information via a physical device or location from protecting the information (BCSI) itself. If the focus is protection of BCSI, the device or storage location becomes less relevant. This is important when considering vendor storage as a service and security considerations regarding physical access and information moving between physical devices outside of the Responsible Entity's direct control. To accomplish this, the focus and means of protection have been shifted to address the possession and utilization of the information. Possession of BCSI addresses physical and electronic/digital controls to protect BCSI. Utilization of BCSI addresses that when BCSI is not in possession, an entity can take precautions to reasonably assure that, if BCSI is compromised from a possession aspect, the BCSI would not be able to be utilized. There are three benefits with moving in this direction:

1) There are different levels of compromise. This provides a more granular way of evaluating and reporting risk during a BCSI compromise. Before this approach, reporting a compromise or mishandling was binary and did not accurately depict risk or the actual ability of a threat actor to capitalize and exploit the information.
2) The focus is now on ensuring controls around BCSI. Physical and electronic controls now become a means to protect how information is possessed and utilized.
3) There is now the ability for the entity to address controls that are independent of possession of BCSI. This will play a significant role in leveraging technologies such as the "cloud."

The SDT also wanted to ensure backwards compatibility with the previous requirement, where feasible. Authorization for electronic and unescorted physical access and access to BCSI must still be based on necessity of the individual performing a work function. Documentation showing the authorization should still have some justification of the business need included. To ensure proper segregation of duties, the same person should still not perform access authorization and provisioning, where possible.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.4
New Requirement R1, Part 1.4, was drafted to allow Responsible Entities to implement a BCSI risk management methodology for vendors that store the Responsible Entity's BCSI and allow a risk-based approach to address the security objectives. One example of a risk-based approach is allowing Responsible Entities to develop their BCSI risk management methodology around risks posed by various vendors involved within the Responsible Entity's BCSI life cycle. This flexibility is important to account for the varying needs and characteristics of Responsible Entities and the diversity of BCSI-related environments, technologies, and risk.

The SDT recognized that CIP-013-1, Requirement R1, can be leveraged to incorporate protection of BCSI but does not currently include information protection.

This requirement includes the following three sub-requirements as a basis for implementing a BCSI risk management methodology:

1) Part 1.4.1 is included so the Responsible Entity will perform an initial risk assessment of any vendor(s) selected to store its BCSI to identify risk factors that could potentially compromise the Responsible Entity's BCSI within the vendor's environment, analyze the risk of the BCSI being compromised, and review the results of the risk analysis.
2) Part 1.4.2 is included so the Responsible Entity will review the vendor(s) that stores its BCSI at least every 15 calendar months to confirm whether the vendor(s) is still the most reliable vendor to perform that function for the Responsible Entity and the Bulk Electric System.
3) Part 1.4.3 is included so the Responsible Entity will document the results from the risk assessments performed in Parts 1.4.1 and 1.4.2 and an action plan to remediate or mitigate risks identified in the assessment.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.5
New Requirement R1, Part 1.5, was transferred from CIP-004-6, Requirement R5, Part 5.3, to consolidate into one Standard both BCSI protection and BCSI access revocation for termination actions within 24 hours.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The requirement to revoke access to BCSI at the time of the termination action still includes procedures showing revocation of access to BCSI concurrent with the termination action. This requirement also still recognizes the timing of the termination action might vary depending on the circumstance.

For applicability, the SDT included Medium Impact BES Cyber Systems with this requirement regardless of whether the Medium Impact BES Cyber System had External Routable Connectivity. The SDT does not

feel that External Routable Connectivity is a determining factor for what the Responsible Entity has identified as BCSI.

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

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R1, Part 1.6

New Requirement R1, Part 1.6, was transferred from CIP-004-6, Requirement R4, Part 4.4, to consolidate into one Standard both BCSI protection and the 15-calendar-month BCSI access review.

The SDT wanted to ensure backwards compatibility with the previous requirement, where feasible. The BCSI privilege review at least once every 15 calendar months is still in place to ensure an individual's associated privileges to BCSI are the minimum necessary to perform their work function (i.e., least privilege). This involves determining the specific roles with BCSI (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access to BCSI does not assume any specific software, and it can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the BCSI privilege review on individual accounts.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column has added language to specify BCSI that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Rationale for New Requirement R2, Part 2.1

New Requirement R2, Part 2.1, was drafted by the SDT to require Responsible Entities to develop a key management process(es) within their information protection programs to restrict access with revocation ability. Key management provides a layer of defense against bad actors who may have the means to physically or electronically obtain BCSI but not use or modify BCSI; this has not been previously required but is needed regardless of the location or state in which the Responsible Entity's BCSI resides. The requirement language includes the minimum expectations for the key management life cycle to guide Responsible Entities while they are developing a key management program and to provide an auditable requirement for Compliance Enforcement Authorities.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6.

Rationale for New Requirement R2, Part 2.2
New Requirement R2, Part 2.2, was drafted to require Responsible Entities to ensure separation of duties in the Responsible Entity's key management process(es) so, regardless of the location or state in which the Responsible Entity's BCSI resides, the risk of unauthorized access to the Responsible Entity's BCSI can be minimized. Controls must be implemented to separate the BES Cyber System Information custodial entity's duties independently from the key management duties established in Requirement R2, Part 2.1. If a Responsibility Entity is unable to implement these controls, and there is a compromise of its BCSI, the time and cost for a Responsible Entity to recover from the compromise of its BCSI could be significant to the Responsible Entity and even to the Bulk Electric System.

The SDT identified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column has been included to accommodate this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.6, and Requirement R2, Part 2.1.

Rationale for Modifications to Requirement R2, Part 2.1 (will become new Requirement R3, Part 3.1)
The SDT combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language under CIP-011-3 Requirement R3, Part 3.1.

In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.

Rationale for Retirement of CIP-011-2 Requirement R2, Part 2.2
The intent of CIP-011-2, Requirement R2, Part 2.2, which is related to BES Cyber Asset disposal, will be addressed in CIP-011-3, Requirement R3, Part 3.1, so CIP-011-2, Requirement R2, Part 2.2, is being recommended for retirement.

Technical Rationale for Reliability Standard CIP-011-2

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-011-2 standard to preserve any historical references.

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:
Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use

classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Protection Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:
This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal of a BES Cyber Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4(CIP-011-3 Requirement R1, Part 1.6) and a portion of Part 4.1(CIP-011-3 Requirement R1, Part 1.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5

The VSL has been revised to reflect the removal of Part 5.3(CIP-011-3 Requirement R1, Part 1). The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-3, Requirement R1

Requirement R1 was revised to include PCA and eliminate potential barriers to use cloud based services for storage of BES Cyber System Information. No changes to the VRF are necessary from the previously approved standard. The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning time horizon to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The requirement has sub-requirements and is assigned a single VRF consistent with other Requirements within the proposed standard.

VRF Justifications for CIP-011-3 R2	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**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	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective, which is to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-011-3, R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during	The Responsible Entity has not documented or implemented any processes for BES Cyber System Information protection (R2)

		storage, transit, use and disposal (Part 1.2)	

VSL Justifications for CIP-001-3, 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 R1 is 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-001-3, 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. The VSL is assigned for a single instance of failing to implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection.

VRF Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R3 (Moved from R2 to R3 in CIP-011-3)
The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 to CIP-011-3

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-011 Requirement R1.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R4, Part 4.1.3 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.3 Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Access to designated storage locations for BES Cyber System Information moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus changed from access to designated storage locations to access to BES Cyber System Information.
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	CIP-011-3, Requirement R1, Part 1.6 Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determines are necessary for performing assigned work functions.	15-month entitlement reviews to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. Focus of verification changed from designated storage locations to BES Cyber System Information.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R4, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	CIP-011-3, Requirement R1, Part 1.5 For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Next calendar day termination actions for those with access to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus of termination actions changed from access to designated storage locations to access to BES Cyber System Information.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-2

BES Cyber System Information (BCSI)-related access management requirements were moved from CIP-004-6, Requirements R4 and R5, to CIP-011-2, Requirement R1. In addition, new requirements have been implemented to mitigate risks associated with BCSI and off-premises vendor services.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.1 Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.	Added requirement language for Responsible Entities to identify designated BCSI storage locations, whether physical or electronic, along with BCSI, which was already required.
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	CIP-011-3, Requirement R1, Part 1.2 Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use and disposal.	Established a stand-alone requirement for authorization of access to BCSI based on need, except for CIP Exceptional Circumstances. This change helps to consolidate all BCSI-related requirements under one CIP Standard. This sub-requirement was carried over from CIP-004-6, Requirement R4, Part 4.1.3. Added the lifecycle element “disposal” to the

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
		requirement to complement actions taken in CIP-011-2, Requirement R2.
CIP-004-6, Requirement R4, Part 4.1.3 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.3 Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Access to designated storage locations for BES Cyber System Information moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus changed from access to designated storage locations to access to BES Cyber System Information.
N/A	CIP-011-3, Requirement R1, Part 1.4 (NEW) Process(es) to identify, assess and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information. 1.4.1 Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and 1.4.2 At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information; and	New CIP-011-3 requirement which is similar to the cyber security risk assessment required as part of CIP-013 Requirement R1. This new requirement is intended to focus risk analysis on potential vendors that will be hosting Responsible Entity's BCSI in the cloud.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	1.4.3 Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	
CIP-004-6, Requirement R4, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	CIP-011-3, Requirement R1, Part 1.5 For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Next calendar day termination actions for those with access to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls. In addition, focus of termination actions changed from access to designated storage locations to access to BES Cyber System Information.
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity	CIP-011-3, Requirement R1, Part 1.6 Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity	15-month entitlement reviews to BCSI designated storage locations moved to CIP-011 to better align with overall Information Protection program controls.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
determines are necessary for performing assigned work functions.	determines are necessary for performing assigned work functions.	Focus of verification changed from designated storage locations to BES Cyber System Information.
N/A	CIP-011-3, Requirement R2 R2. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.1 (NEW) Where applicable, develop a key management program to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage	New CIP-011-3 requirement that leverages NIST 800-57 security controls. The security of BES Cyber System Information protected by obfuscation directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. Key management provides the foundation for the secure generation,

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	2.1.5 Key protection 2.1.6 Key-periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	storage, distribution, and destruction of keys.
N/A	CIP-011-3, Requirement R2, Part 2.2 (NEW) Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	New CIP-011-3 requirement that requires implementation of controls that ensure the separation of duties and organizational independence between the programs used to restrict the ability to obtain BCSI from those programs used to restrict the ability to use BCSI.
CIP-011-2, Requirement R2, Part 2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems"	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber	Combined CIP-011-2, Requirement R2, Part 2.1 (reuse) and CIP-011-2, Requirement R2, Part 2.2 (disposal) within the same requirement language.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Asset data storage media shall be sanitized or destroyed.	In addition, the phrase "that contain BES Cyber System Information" was removed from the requirement language effectively expanding applicability of sanitization or destruction practices to all Applicable Systems, not just those containing BCSI. This was done to align with the historical intent of CIP-007-3 Requirement R7 where reliability data was required to be sanitized as well from Cyber Assets before reuse or disposal.
CIP-011-2, Requirement R2, Part 2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	CIP-011-3, Requirement R3, Part 3.1 Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the "Applicable Systems" column), the Cyber Asset data storage media shall be sanitized or destroyed.	As above. CIP-011-2, Requirement R2, Part 2.2 was combined into CIP-011-3, Requirement R3, Part 3.1.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through February 3, 2020
Ballot Pools Forming through January 20, 2020

Now Available

A 45-day formal comment period for **Project 2019-02 BES Cyber System Information Access Management** is open through **8 p.m. Eastern, Monday, February 3, 2020.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Linda Jenkins. 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. - 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 Standards and Implementation Plan, along with non-binding polls for each associated Violation Risk Factors and Violation Severity Levels, will be conducted **January 24 – February 3, 2020.**

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

For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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:	2019-02 BES Cyber System Information Access Management
Comment Period Start Date:	12/20/2019
Comment Period End Date:	2/3/2020
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 IN 1 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 IN 1 ST 2019-02 BES Cyber System Information Access Management Implementation Plan IN 1 OT

There were 91 sets of responses, including comments from approximately 209 different people from approximately 131 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

2. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

3. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

4. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms "obtain" and "use" in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

5. The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

6. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

7. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

8. The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

9. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

10. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

11. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

12. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

13. Do you have any other general recommendations/considerations for the drafting team?

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	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
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					Bobbi Welch	Omaha Public Power District	1,3,5,6	MRO

					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Bobbi Welch	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1	4	WECC

Snohomish County PUD No. 1						of Snohomish County		
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Long Duong	Public Utility District No. 1 of Snohomish County	1	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
					Jennifer Brey	Arizona Electric Power Cooperative	1	WECC
					Joseph Smith	Prairie Power , Inc.	1,3	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		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
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	PG&E	PG&E	1	WECC
					PG&E	PG&E	3	WECC
					PG&E	PG&E	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no NextEra	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

					Shivaz Chopra	New York Power Authority	5	NPCC
					Mike Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Portland General Electric Co.	Ryan Olson	5		PGE Group 2	Angela Gaines	Portland General Electric Co.	1	WECC
					Dan Zollner	Portland General Electric Co.	3	WECC

					Daniel Mason	Portland General Electric Co.	6	WECC
					Ryan Olson	Portland General Electric Co.	5	WECC
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
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

I don't see the referenced changes in CIP-004-7. If you are refering to CIP-011-3, "storage locations" is very broad. This could be a problem during audits, if the auditor does not like the interpretation. We need a much stricter wording for storage locations.

Likes 1	Miller Scott On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1;
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

It is already implied in CIP-004 R4 that storage locations have to be identified and adds to the complexity of the compliance requirement. Flexibility is already provided under CIP-004 R4. Access controls were grouped in CIP-004 R4, relocating these controls to CIP-011 creates additional complexities.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

An overarching problem with this proposed draft of CIP-011-3 is the removal of the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2.

Identifying BCSI storage locations for system information pertaining to Medium Impact BES Cyber Systems without ERC is not necessary, as Cyber Systems without remote connectivity can only be compromised locally by a breach of physical security. The information protection mandated by this standard will afford no protection should an adversary gain physical access to the Cyber Systems.

We will not be able to vote affirmative unless “with ERC” is added to the Applicability of of Medium Impact BES Cyber Systems in R1 Part 1.1.

We agree that the language provides flexibility in identifying BCSI storage locations.

We would prefer to retain the less prescriptive “Method(s)” over the proposed requirement change to “Process(es).” Making this change to “process” implies that existing programs will need to be updated to a procedural format. Again, this is not requested by the SAR and does not increase reliability, yet this would add administrative burden and increase compliance risk.

To clarify location with respect to electronic storage locations, recommend the definition of “BCSI Repository” per EEI comments along these lines:

“BCSI Repositories are either physical or electronic storage locations where BCSI is retained for long term storage. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location. Short term storage locations for working copies are not part of this definition.”

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Although the proposed revision explicitly states the requirement to identify specific BCSI storage locations, it does not add any actual new flexibility about designating BCSI storage locations. The same flexibility exists today between the lines of existing CIP-004 and CIP-011. It is just implicit, rather than explicit. The confusion remains about the necessity (or lack thereof) to store BCSI in designated BCSI storage locations, how large a collection of BCSI has to be to warrant a BCSI storage location of its own, or how long BCSI can be in use outside of a storage location without creating security and compliance concerns.

Seattle City Light believes a more effective approach would be to clearly state a security objective (“to prevent unauthorized access to BCSI”), require an entity to develop a risk-informed BCSI security plan to achieve this objective, and then require implementation and periodic review of the BCSI security plan. Beyond this, almost all details about specific approaches for and elements that might be expected in a BCSI security plan should be provided in the measures and/or technical guidelines. A few specific elements of the security plan might be requested as sub-requirements, such as i) how to identify BCSI; ii) controls to limit unauthorized access to BCSI in use, transit, and storage; and iii) security requirements expected of third party that uses and/or stores BCSI for the entity, if an entity chooses to employ such parties. Note that by iii) Seattle does NOT mean that any specific security requirements for third party providers should be spelled out as requirement in the revised Standard, but rather than each entity should develop its own risk-based list of the security controls/requirements it demands of any third party provider it may employ with regard to BCSI. And that such entity-specific control requirements would only be required if an entity elected to use third-party BCSI providers. Guidance as to what these requirements might be could be provided in the Measures or supporting technical document.

If a more prescriptive approach to controls is desired, Seattle shares the same concerns expressed by Sacramento Municipal Utility District (SMUD) regarding the change of language about BCSI storage locations.

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

‘System Information pertaining to’ in the applicability column may broaden scope expectations and should be removed.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

We support the overall effort. However, we do not support introducing "System information pertaining to" in the applicability section. This creates some ambiguity. We believe that the applicability should be limited to BCSI.

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 draft language in present form would obligate entities to establish a Data Loss Prevention program to fully satisfy this requirement. This doesn’t support the scope or intent of the original SAR. This goes far beyond controlling access to BCSI and includes topic that may cover how an individual may handle that information (replication, forwarding, etc.). The previous version included the term “Designated repository” for identification of scope of protection. Removal of this qualification creates an obligation to manage BCSI regardless of where it may occur.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

As written the requirement may require the Registered Entity (RE) identify the physical locations a third-party provider is storing the RE's BCSI. We think that it would make more sense to identify the access controls and methods the RE has in place controlling the ability to obtain and use the information.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	No
Document Name	

Comment

AEP agrees with EEI's comments and requests clarification on the requirement to identify BES Cyber System Information (BCSI) storage locations as proposed by the Standard Drafting Team (SDT) for CIP-011-3, Requirement R1, Part 1.1. As written, this requirement would require registered entities to work with their third-party cloud-based service providers to identify the physical location where their BCSI resided on the service provider's cloud-based network. This would be difficult (or possibly impractical) for entities to maintain suitable records on an ongoing basis.

Also, from a compliance perspective, registered entities would have difficulty proving that they granted or removed access to BCSI, as required in the proposed draft for CIP-004-7. To resolve this concern, we suggest that the SDT modify the proposal to require registered entities to prove access is granted or removed to a BCSI Repository.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA does not support the replacement of the term “method” with the term “process.” A “method” for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process) to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Additionally, NRECA does not support the addition of a requirement to “identify applicable BES Cyber System Information storage location.” The Technical Rationale indicates that the SDT wanted to shift focus from the storage location to the information; however, this addition places the focus back on to the storage location for what appears to be solely administrative purposes. As well, the description of what was intended for identification in the Technical Rationale exceeds the scope of the verbiage added to Requirement R1.1. Identification of an object is different than description of an object and the requirement language addresses only the former while the Technical Rationale is clearly suggesting the latter. Thus, this addition creates ambiguity and confusion regarding Responsible Entity’s obligations for little or no benefit to BES reliability.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

The addition of a new requirement is not necessary because 1) REs already have the flexibility to identify BCSI storage locations, and 2) None of the rest of the proposed requirements reference storage locations anyway.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC does not support the replacement of the term “method” with the term “process.” A “method” for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process)

to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Additionally, GSOC does not support the addition of a requirement to "identify applicable BES Cyber System Information storage location." The Technical Rationale indicates that the SDT wanted to shift focus from the storage location to the information; however, this addition places the focus back on to the storage location for what appears to be solely administrative purposes. As well, the description of what was intended for identification in the Technical Rationale exceeds the scope of the verbiage added to Requirement R1.1. Identification of an object is different than description of an object and the requirement language addresses only the former while the Technical Rationale is clearly suggesting the latter. Thus, this addition creates ambiguity and confusion regarding Responsible Entity's obligations for little or no benefit to BES reliability.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

SMEC also disagrees with the removal of the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO agrees in principle with the comments submitted by NPCC:

1. We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc.
2. For the Applicability column referencing "system information," we suggest changing "System information pertaining to:" to "Information associated with," or clarification of what is considered "system information"
3. We recommend clarifying by stipulating that the Entity's information protection plan includes a description of the storage location(s) and that the Entity maintains a list of those storage locations

4. It is unclear if the intent of R1.1. is also for an entity to *develop a process* to list the storage locations or the actual inventory list of the storage locations. If the intention is not a “process”, then subdivide 1.1 requirement into two component parts: 1.1.1 a process to identify what constitutes BCSI and 1.1.2 a second requirement to have an inventory of locations.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

No, the current version of CIP-004 already provides for the identification of BCSI storage locations. Keeping all the requirements for access and revocation in one standard decreases the complexity for compliance.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The SDT should consider that with cloud computing the physical location of BCSI is irrelevant. It is more important to protect the data vs where the data is located. Cloud computing currently replicates data in data centers world-wide. Entities will not be able to verify where cloud BCSI exists.

This is duplicative in nature. The requirement to approve access by itself requires entitites to know where the data is located. Hence authorization though roles or entitlments identifies the locations of the BCSI.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	
Comment	

With respect to Applicability, the term 'System Information" is undefined. Perhaps the team intended to include "BES Cyber System Information" In any case, greater clarification of this term is needed.

The term "Method" allows the Registered Entity greater flexibility to provide guidance to meet the intended security objectives of the requirement. In that regard, I do not agree that the use of the term "process" is a better choice for this requirement as this implies a rigid step-by-step structure.

With respect to the Measure concerning "Indications on information.....", the language should be clarified to permit classification of the electronic storage location as contaning BCSI and not each individual document or file while at rest within that access-controlled location. Indications should be considered for data in transit.

I agree that a listing of individual storage locations for BCSI should be identified and maintained.

Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	
Comment	

New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information.

Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	
Comment	

‘System Information pertaining to’ in the applicability column may broaden scope expectations and should be removed.

Likes 1	Barry Jones, N/A, Jones Barry
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 1	Barry Jones, N/A, Jones Barry
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	No
Document Name	

Comment

New R1.1 still stresses “Identify applicable BES Cyber System information storage locations.” According to the SAR, the emphasis was supposed to move away from storage “locations” and focus on the protection of the information itself. However, to maintain security of information being stored outside of a Registered Entity using cloud services and vendors, to conform to the SAR, and without imposing undue regulatory burdens to entities using encryption key management for BCSI stored within the Responsible Entity, the language should be modified to say “Identify applicable BES Cyber System information storage locations *not owned or managed by the Responsible Entity.*”

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.”

We agree with EEI’s suggestion to create the new term “BCSI Repository” to better define BCSI storage locations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	
Part 1.1 as written requires a process for identifying two things; BCSI and BCSI storage locations. However there is no other mention of BCSI storage locations within the standard. Since there are no proposed requirements for these storage locations, a process to identify them has no function. The remainder of the requirements apply to the BCSI as identified in R1.1 with no further mention of the storage locations. We are concerned with the philosophical shift from BCSI storage locations as the object of many of the requirements to the BCSI itself, in particular all the requirements that were previously in CIP-004. Managing and auditing access to BCSI as simply information in whatever form and wherever it is being used is an infinite scope. In order for access to be managed and audited, it must have finite and discrete objects such as designated BCSI storage locations. For example, entities will be unable to prove compliance with CIP-011 (R1.3 and R1.5 in particular) on BCSI as it exists in the form of a working copy of a printed network diagram used by a technician in a substation to troubleshoot a communications issue. By making BCSI the object of the requirements rather than the designated storage locations, the scope has been expanded to a point that is unmanageable and unmeasurable with which entities are unable to prove compliance. We suggest the object of the requirements remain as they were in CIP-004 and explicitly reference designated BCSI storage locations as their object, not simply BCSI.	

Also, the requirement does not “allow an entity the flexibility” to identify storage locations for BCSI, it requires that an entity do so. The identification of storage locations containing BCSI is, for all practical audit purposes, already required under CIP-011-2 (See the NERC Evidence Request Tool, BCSI Tab), and the proposed wording does not allow any flexibility – it explicitly requires an entity to develop and maintain a list.

The applicability of Part 1.1 has changed to “System information pertaining to…”, which raises a concern over what “system information” is and how does an entity prove they have performed their BCSI identification process on the universe of all such information? We are concerned that “system information” is not a finite or discrete scope for this requirement. A requirement with a stated applicability of all possible information about a system is a showstopper issue.

Southern suggests that instead it should require a process for determining BCSI for high/medium impact BCS. An example replacement R1 that is not in “table format” could state “Each Responsible Entity shall have a process to identify BCSI that pertains to high impact or medium impact BCS and their associated EACMS and PACS.” Subsequent R2, R3, etc. could then outline the necessary parts of the information protection program scoped to that identified BCSI.

If keeping the table format for R1 is desired, retaining the the high/medium impact BCS as the applicability of Part 1.1 and then require “Processes to identify BCSI that pertain to the applicable systems” is preferable. It should stay scoped to high/med impact BCS and not the full universe of system information.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

In addition, as an alternative to EEI’s proposed definition for BCSI Repository, SDG&E tenders its alternate definition below:

BCSI Repository – Either a physical or electronic storage location where BES Cyber System Information is stored, and for which access is controlled. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	

1. We would recommend security objectives (similar to CIP-013-1) instead of prescriptive requirements. Information protection program should include identification, access control, etc.
2. We suggest changing “System information pertaining to:” to “Information associated with,” or clarify the term “system information”.

Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.

However, we share the concerns expressed by EEI.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, "and identify applicable BES Cyber System Information storage locations." Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the 'Applicability' as Part 1.1, but add, "with ERC" to Medium Impact BES Cyber Systems, and in the Requirement section, "Method(s) to identify applicable BES Cyber System Information storage locations." This could in turn be changed to "Method(s) to identify applicable BES Cyber System Information Repositories" per the EEI recommendations.

We agree with EEI's suggestion to create the new term "BCSI Repository" to better define BCSI storage locations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

Our first suggestion is that the Applicability for 1.1 be returned to it's original state without any additional conditions or prerequites. Absent that,

1. We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc.

2. Since we have some debate over “system information,” we suggest changing “System information pertaining to:” to “Information associated with,” or clarification of “system information”. At a minimum, if “system information” must be used. It should be established as a NERC glossary Defined Term.

3. We recommend clarifying by stipulating that the Entity’s plan includes a description of the storage location(s) and maintains a list of those storage locations.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

The SAR stressed that changes would be focused on “…BCSI and the ability to obtain and make use of it”, where the current standard “…focused on access to the ‘storage location’…”, yet the proposed changes add additional requirements to identify the storage locations. This seems to be contrary to the main objective of the SAR. We have additional concerns about what the SDT means about storage location and how it pertains to storage at vendors and their networks. We suggest that the SDT clarify what their intent was regarding the changed requirement on storage location.

Additionally, the proposed changes add PCAs as applicable systems, which by definition do not contain BCSI. It seems that this addition is outside of the SAR and it would be helpful for the SDT to describe how adding this “clarifies the protections expected when utilizing third-party solutions”. We believe that no changes are needed to R1 Part 1.1 to address the SAR and thus, the current language should remain the same.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments: MISO agrees the changes are necessary; however, we also have concerns. As the existing language in CIP-004-6, requirement R4, part 4.1.3 implies and/or can be interpreted as limiting access to the storage location as opposed to controlling access to BCSI regardless of location, MISO supports adding language to require identifying information and applicable BCSI storage locations will expand flexibility and options.

That said, MISO proposes the SDT more clearly articulate the following key distinctions raised during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020: physical or electronic, responsible entity or vendor hosted. To make this clear in the proposed standard, MISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows:

"Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity's information protection program"

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy Houston Electric, LLC (CEHE) supports the comments as submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI member companies (EEI) identified four issues for further consideration by the SDT and proposes solutions to address some of those issues.

First, EEI urges the SDT to clarify the requirement to identify BES Cyber System Information (BCSI) storage locations as proposed by the SDT for CIP-011-3, Requirement R1, Part 1.1. The requirement, as written, requires registered entities to work with their third-party cloud-based service providers to identify the physical location where their BCSI resided on the service provider's cloud-based network. The challenge is the difficulty and, potential impracticality for entities to track down and maintain records from service providers to demonstrate compliance on a continuing basis. To address this challenge, the SDT should clarify BCSI "Storage Location" and address electronic and physical repositories within that definition. As an alternative, EEI suggests the SDT define the term "BCSI Repository," which would provide registered entities a simpler solution than what was provided in the proposed revisions to CIP-004-7 and CIP-011-3. Additionally, EEI offers the following definition for SDT review and consideration:

BCSI Repository – Either a physical or electronic storage location where BES Cyber System Information is retained. For physical BCSI Repositories, this would be a physical location. For electronic BCSI Repositories, this would be a logical location. **Notes:** *Issues surrounding short term storage of BCSI (e.g., working copies, etc.) are not intended to be part of this definition but would need to be addressed by responsible entity's policies and procedures.*

Second, to provide clarity with respect to the applicability of Requirement R1, Part 1.1., EEI suggests replacing the undefined term, "system information" with the NERC defined term, "BES Cyber System Information."

Third, the SDT's proposal creates compliance challenges. Registered entities would have difficulty proving the granting and removal of access to BCSI as contemplated in the proposed draft for CIP-004-7. As an alternative, EEI suggests using the BCSI Repository definition shown above, and revising proposed CIP-004-7 to require registered entities to prove access and removal of access to a BCSI Repository.

Fourth, EEI is concerned that the SAR scope may have expanded without providing necessary justification within the Technical Rationale. See our comments to Questions 11 below.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO felt that the changes are necessary. The existing language in CIP-004-6, requirement R4, part 4.1.3 implies and/or can be interpreted as limiting access to storage location options as opposed to controlling access to BCSI regardless of location. By adding language to require identifying information coupled with an identification of applicable BCSI storage locations would certainly add acceptable options and provide a responsible entity flexibility in choosing technology solutions.

In addition, NYISO feels that the SDT more clearly articulated key distinctions during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar that was hosted on January 16, 2020. In order to make this clearer, NYISO would suggest that the SDT should endeavor to expand the language of the last example in the current draft provided under requirement R1, Part 1.1, Measures as follows:

"An inventory of locations, either physical or electronic, either housed within a responsible entity's data center or vendor hosted that are identified as housing the responsible entity's BES Cyber System Information be a part of the entity's information protection program"

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 NextEra	
Answer	No
Document Name	

Comment
1) We recommend security objectives instead of prescriptive requirements. Information protection program should include identification, access control, etc. 2) Since we have some debate over “system information,” we suggest changing “System information pertaining to:” to “Information associated with,” or clarification of “system information”. 3) We recommend clarifying by stipulating that the Entity’s plan includes a description of the storage location(s) and maintains a list of those storage locations.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment
The requirement is not necessary. Why should we have to identify our locations to NERC? There should be security objectives instead of prescriptive requirements.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	

Comment

SNPD is concerned that the proposed wording INCREASES rather than DECREASES ambiguity. The current language is understood to require Entities to designate BCSI storage locations, which is the fundamental security imperative to enable proper access control. Semantics between terms such as “designate” vs. “identify” or another synonym will not fundamentally alter how Entities choose to interpret and respond to R1. There are already substantial differences between how Entities interpret the current language. In other words, the current wording is descriptive and defines the imperative.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with NSRF and EEI’s comments.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

The approach of identifying the storage locations is welcomed since this is where controls are applied and is compatible to current CIP-004 requirements. The drafting team needs to avoid requirements that can be interpreted as requiring protection of each individual piece of BCSI.

It would be helpful to clearly define what is meant by “storage locations”. Is it geographical? Is it the server or tenant with a cloud provider? This distinction could be important when BCSI is housed by a vendor or other third-party. Consider adding identification of a) storage locations with the entity, b) with a vendor who provides custom services with identified personnel for in scope cyber systems or assets and c) with a certified cloud service provider who provides generic cloud based services without insider knowledge.

The Applicability column needs to be modified to limit the information to only BCSI, and not all system information pertaining to the system categories listed. Just using “system information” will cast too wide of a net on identifying BCSI. Consider revising as, “BES Cyber System Information for:” This is easily understood since it is a defined term with defined criteria.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2

Answer	No
Document Name	

Comment

PGE agrees with EEI’s comments

Likes 1	Portland General Electric Co., 3, Zollner Dan
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike

Answer	No
Document Name	

Comment

No, The term “designated storage locations” offered additional clarity that it was only those storage locations designated as such by the responsible entity that would meet this requirement. However, the updated term “applicable BES Cyber System Information storage locations” offers no clarity of

which storage locations would be applicable. This could have the unintended consequence of increasing the scope of locations to be managed under CIP. The term is too broad, and should be left as “designated storage locations” or amended to “designated storage locations of BCSI.”	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
The requirement is not necessary. Why should we have to identify our locations to NERC? There should be security objectives instead of prescriptive requirements.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations.	

However, we share the concerns expressed by EEI and the MRO NSRF.

While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows:

In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet.

Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.” This could in turn be changed to “Method(s) to identify applicable BES Cyber System Information Repositories” per the EEI and MRO NSRF recommendations.

Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The approach of identifying the storage locations is welcomed because this is where controls are applied, and the approach is compatible to current CIP-004 requirements. ERCOT suggests the drafting team avoid requirements that can be interpreted as requiring protection of each individual piece of BCSI.

ERCOT believes it would be helpful to clearly define what is meant by “storage locations.” Is it geographical? Is it the server or tenant with a cloud provider? This distinction could be important when BCSI is housed by a vendor or other third-party. ERCOT suggests the drafting team consider adding identification of (a) storage locations with the entity, (b) vendors that provide custom services with identified personnel for in scope cyber systems or assets, and (c) certified cloud service providers that provide generic cloud based services without insider knowledge.

The Applicability column should be modified to limit the information to only BCSI, and not all system information pertaining to the system categories listed. Just using “system information” may cast too wide of a net on identifying BCSI. ERCOT suggests the drafting team consider revising to read “BES Cyber System Information for:” This would likely be more easily understood because it is a defined term with defined criteria.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1,

3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E does not agree with required identification of BCSI storage locations. The stated purpose and emphasis of the modifications is the protection of “System Information” (i.e. BCSI) and PGAE does not believe that this burdensome requirement enhances protection of BCSI. The requirement to identify storage locations has been administratively burdensome and challenging for BCSI placed on internal servers but could be impossible for BCSI placed on third-party provider infrastructure (i.e. cloud), especially if the service providers have the capability to store the BCSI on multiple instances of their infrastructure for redundancy and resilience. PG&E recommends the required identification of storage locations be removed while maintaining the emphasis on the protection of the BCSI.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
The change from "designated storage locations" to "applicable ... storage locations" increases the confusion that already surrounds this topic.	
Likes 0	

Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	

Comment
Yes, we agree that the language in R1 Part 1.1, as written, allows the Responsible Entity the flexibility in identifying BCSI storage locations. However, we share the concerns expressed by EEI and the MRO NSRF. While the requirement is necessary, we do propose splitting R1 Part 1.1 into two parts as follows: In Part 1.1: change the Requirement to delete the phrase, “and identify applicable BES Cyber System Information storage locations.” Also, in the Measures, delete last bullet. Recommend creating a new Part 1.2: with the ‘Applicability’ as Part 1.1, but add, “with ERC” to Medium Impact BES Cyber Systems, and in the Requirement section, “Method(s) to identify applicable BES Cyber System Information storage locations.” This could in turn be changed to “Method(s) to identify applicable BES Cyber System Information Repositories” per the EEI and MRO NSRF recommendations. Applicability of current R1 Parts 1.3 to 1.6, and R2 Parts 2.1 and 2.2, change to reference a newly created R1 Part 1.2

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	

Comment
We recommend clarifying the requirement by stipulating that the Entity’s plan includes a description of the storage locations for BCSI and maintains a list of those storage locations. In addition, there should be language describing what is meant by “storage locations.” The definition is important when

BCSI is housed by a vendor or other third-party. Finally, the requirement should cover only BCSI and not all system information pertaining to the system categories listed in the Applicability column. Accordingly, “system information” in the Applicability column should be changed to the defined term “BES Cyber System Information.”	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
In its current form, CIP-004 and CIP-011 already provides flexibility. The current requirements to address access to sensitive data and information seem acceptable in the current formats. What is unclear is how the BCSI will be usable if it must always reside in specific locations? For example, is it violation if someone who has access, temporary pulls that information off the stored location and prints the document for review? While a copy of that data is stored in the storage location, the hard copy now creates an issue. What happens when that person takes it outside the physical security perimeter? Entities should be required to describe how they identify BCSI, how BCSI is transmitted, whom may have access to the data and information, the description electronic access controls, and how exceptions, if any, exist in relation to the use of the information outside of those parameters. The real issue is where it is stored. Auto saves, inadvertent machine shutdowns, etc. may cause the data to be stored in a location outside the acceptable storage location. Virtualization, Office 365, etc. may cause issues for entities to be able to ensure the information is never stored outside of a set storage location. While SunPower believes there can be adequate controls, the programs and systems industry use will likely cause an increase of possible violations as those programs and systems change by the provider. Temporary storage on local devices that are also secured by an approved user should be allowed, at least on a temporary basis.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
While the requirement seems flexible, it is subject to confusion in implementation. The previous version specificially identified electronic or physical controls. This version extends scope to include the cloud. However, in doing so, it removes the context for full understanding of the requirement. Lacking this context, there is a signficant potential of having multiple interpretations of the requirement.	
Likes 1	Miller Scott On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1;
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: We feel the language could be clearer if the BES Cyber System itself was excluded being it is already being protected by the NERC CIP requirements. The same problem exists within the standard today. It does not exclude BCSI contained within the BES Cyber System itself. Although it is inherent BES Cyber Systems contain BCSI, the standards do not exclude those systems/Cyber Assets from containing BCSI, thus the Cyber Assets themselves would be BCSI repositories and should be documented as such. We have not seen this as a problem in audit, but a strict auditor could make this an issue the way it is written. Also, examples of potential Cyber Assets containing BCSI could be better expanded in the Guidelines and Technical Basis, such as SIEMs, Anti-virus servers, backup servers, etc. which are not a part of a BES Cyber System and the rationale behind why they are or are not considered BCSI repositories.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees that CIP-011-3 R1, Part 1.1 allows flexibility to identify which storage locations are for BCSI and agree the requirement is necessary.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

While we agree that including the need to identify storage locations, this could prove burdensome to entities. Identification of a location in cloud storage providers (e.g. OneDrive, Microsoft Teams, Sharepoint, etc.) which offer seamless creation and storage of documentation may make it difficult to identify specific storage locations. This could result in entities not listing key storage locations or generalizing, at a loss of security, in order to meet the requirement.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	Yes
Document Name	

Comment

There is more than one question and we vote yes on the first question and no on the second. There should only be one quetion, not two.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County

Answer	Yes
Document Name	

Comment

Yes, due to improved applicability and exclusion of low impact assets.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment

Agree with adding requirement to identify BCSI storage locations even though it is already

Implicitly required to be identified in CIP-004-6 R4.1. To better identify BCSI storage locations, we

would suggest making a definition of BCSI Repository as follows:

“A multi-user electronic or physical locations where a collection of BCSI is retained for long-term

storage.”

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

We feel the language could be clearer if the BES Cyber System itself was excluded being it is already being protected by the NERC CIP requirements. The same problem exists within the standard today. It does not exclude BCSI contained within the BES Cyber System itself. Although it is inherent BES Cyber Systems contain BCSI, the standards do not exclude those systems/Cyber Assets from containing BCSI, thus the Cyber Assets themselves would be BCSI repositories and should be documented as such. We have not seen this as a problem in audit, but a strict auditor could make this an issue the way it is written.

Also, examples of potential Cyber Assets containing BCSI could be better expanded in the Guidelines and Technical Basis, such as SIEMs, Anti-virus servers, backup servers, etc. which are not a part of a BES Cyber System and the rationale behind why they are or are not considered BCSI repositories.

Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST suggests changing: “Process(es) to identify information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations” to “Process(es) to identify information that meets the definition of BES Cyber System Information and to identify BES Cyber System Information storage locations.”	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE recommends revising “System information” to “Information” in the Applicability column to be consistent with the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 1	NiSource - Northern Indiana Public Service Co., 3, Bazylyuk Dmitriy
Dislikes 0	
Response	

2. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

Bradley Collard - SunPower - 5

Answer	No
Document Name	

Comment

It appears the scope has greatly expanded. Because of the focus of all possible BCSI storage locations, entities will not only be focused on who should have access and how access is controlled, but where that information may be stored temporally and where it might be duplicated.

Additionally, how are Cloud storage services handled in the new CIP-011-3? The physical security perimeter of that service exists outside of the control of the registered entity.

If, during a CIP Exceptional Circumstance, information is transmitted to another person to help facilitate an issue, at the end of the CIP Exceptional Circumstance, data cleanup becomes a problem.

Are entities to identify the RE file server location if an entity is required to send a Regional Entity BCSI?

The focus should be access controls, as the long-term storage is already considered in that process.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

Comments: No. The CIP-004-6 requirements are based on an “Applicable System” approach and access to BCSI designated electronic and physical storage locations. However, CIP-011 shifts the paradigm to “Applicability,” access to BCSI, and the ability to obtain and use the information.

Recommendation: Ensure that the implementation timeline accounts for the need to shift the construct of an Entity’s information protection program.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

By moving the requirements from CIP-004 to CIP-011 will require a reworking of existing evidence and will cause confusion during any subsequent audits.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We support the EEI and MRO NSRF comments that disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

Likes 0	
Dislikes 0	

Response

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	No
Document Name	

Comment

"Method(s) to prevent the unauthorized access to and use of BES Cyber System Informatin during storage, transit, use, and disposal." is a practical than "elminate the ability to ...."

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

We support the EEI and MRO NSRF comments that disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I don't see backwards compatibility based on the methods listed in 1.2.	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
No, The term “designated storage locations” offered additional clarity that it was only those storage locations designated as such by the responsible entity that would meet this requirement. However, the updated term “applicable BES Cyber System Information storage locations” offers no clarity of which storage locations would be applicable. This could have the unintended consequence of increasing the scope of locations to be managed under CIP. The term is too broad, and should be left as “designated storage locations” or amended to “designated storage locations of BCSI.”	

Additionally, the CIP-004-6 access level requirements were scoped to High Impact BCS, and Medium Impact BCS with ERC. The CIP-011 replacement broadly expands the scope of the access level requirements.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
All BCSI access requirements should remain under CIP-004 as one Standardized Security Standard (centralized location). Leaving the BCSI access with cyber and physical provides a holistic security access management and review program verses fragmenting access management.	

Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD is concerned that the proposed wording INCREASES rather than DECREASES ambiguity. The current language is understood to require Entities to designate BCSI storage locations, which is the fundamental security imperative to enable proper access control. Semantics between terms such as "designate" vs. "indentify" or another synonym will not fundamentally alter how Entities choose to interpret and respond to R1. There are already substantial differences between how Entities interpret the current language. In other words, the current wording is descriptive and defines the imperative.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
I don't see backwards compatibility based on the methods listed in 1.2.	

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO's response is based on the assumption this question relates to the proposed changes in CIP-011-3 within requirement R1, parts 1.3, 1.5 and 1.6.

NYISO believes that the proposed changes maintain backwards capability. That said, the proposed changes in CIP-011-3 also introduce a potential complication; having to maintain similar access authorization, revocation and control measures as that currently contained within CIP-004-7. This could create a situation whereby a single deficiency in an entity's access management program could lead to potential non-compliance with two separate NERC standards.

Note – during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020*, the SDT explained that their intent in proposing these modifications was to direct the content of CIP-004-7 solely on BCS while focusing the content of CIP-011-3 solely on BCSI.*

NYISO recognizes and agrees with the SDT's intent to consolidate similar issues. Our recommendation would be for the SDT to maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. In addition, NYISO would also propose that the SDT consider similar treatment of vendor related risk assessment requirements be incorporated and consolidated within CIP-013-2.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI appreciates the considerable efforts of the SDT to streamline Requirements associated with BCSI within the proposed changes to CIP-004-7 and CIP-011-3. However, EEI is concerned that the proposed changes may create a situation where responsible entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards. For example, if an entity developed a process to remove access to BCSI, including other logical access, and there was a failure in that process, the proposed requirement could be interpreted as a violation of CIP-004-7 R5 and CIP-011-3 R1. Whereas, under the current approved standards this situation would result in a single violation of CIP-004-6 R5.

Likes 0	

Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree that there is a minimal effort to meet the proposed obligations due to the addition of PCAs. Adding the phrase, “System information pertaining to:” in the Aplicability column does provide greater clarity between BCSI and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO’s response assumes this question relates to the proposed changes in CIP-011-3, requirement R1, parts 1.3, 1.5 and 1.6. MISO believes the proposed changes maintain backwards capability; however, the proposed changes in CIP-011-3 also introduce a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. This could create a situation whereby a single deficiency in an entity’s access management program could lead to potential non-compliance with two NERC standards at the same time. *Note – during the* Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020*, the SDT explained their intent in proposing these modifications is to focus the content of CIP-004-7 solely on BCS and the content of CIP-011-3 solely on BCSI.* MISO recognizes and agrees with the SDT’s intent to consolidate similar issues. We recommend that the SDT maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. Likewise, MISO would propose the SDT consider similar treatment of vendor related requirements by incorporating them into CIP-013-2.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No

Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
While we understand the reasoning behind including access to BES Cyber System Information storage locations in CIP-011, the 2016-02 SDT made great efforts to consolidate like requirements together and remove the “spaghetti” requirements. We believe that these changes are undoing that effort. The ability for an entity to have a single access management program (dealing with physical, electronic and information access) provides economy of scale and less opportunities for mistakes or confusion. While we do believe these changes maintain backwards compatibility, we cannot support splitting access management into multiple Standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	

Answer	No
Document Name	
Comment	
NYPA believes that some backward compatibility has been lost since the modified Standard has been modified to extend to ALL Medium Impact BES Cyber Systems	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the EEI comments that disagree with the qualifying language "with ERC" dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards. *Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.*	

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a sufficient protection.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
We do appreciate the SDT concern with backwards compatibity, but since we are recommending changes to the current drafts of CIP-004-7 and CIP-011-3, we are not able to agree at this time.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	

SDG&E supports EEI's comments submitted on our behalf.

SDG&E would like to additionally speak to the new draft standard R1.3 requirement of "Process(es) to authorize access to BES Cyber System Information…" The existing requirements require authorization for the repositories that BCSI is stored in. A change to authorizing access to BCSI generally will be a large deviation from current practices and creates many questions about how to authorize/track access to each piece of BCSI.

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

We do not agree as one of the fundamental concepts of CIP-004 R4 Part 4.1.3 that was lost in the proposed transition to CIP-011 R1 Part 1.3 is the difference between authorizing access to *BCSI storage locations,* which is a discrete and finite object that can be monitored and audited (the current CIP-004 approach), while the new CIP-011 approach is *access to BCSI* wherever and however it exists inside or outside of its storage locations (i.e. a hardcopy of a network diagram in a company truck). This fundamental change has made the requirement unmeasurable and non-auditable. We believe the primary issue of hardware or device level requirements that prevented the use of cloud services was in CIP-011 R2 that required data destruction at a Cyber Asset/physical storage media level. We do not agree with moving the authorization programs away from BCSI *storage locations*. A "storage location" can be a designated encrypted area on a cloud service.

Additionally, we do not agree with moving the "access management" requirements for BCSI out of CIP-004-6 and into CIP-011-3. Although one argument is to keep all requirements applicable to BCSI in a single standard, the same argument could be applied to keep all "access management" requirements in the same standard. This is additionally supported by the fact that this is how all entities have currently structured their compliance programs, and the justification to reallocate those requirements to CIP-011-3 causes more undue burden than any resultant benefit.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes this is not a minimal effort. There is a difference between access to a location and consuming information stored in that location. The need to know standard is not contained in the verbiage of the requirement, but is in the guidance. Need to know implies consuming the information while need to access is simply controlling access. The need to know standard for actually consuming and using information is an unsustainable burden at remote, especially rarely occupied, locations and could interfere with the ability to perform operations in an emergent situation. All personnel with access to storage locations have authorization; those who do not actually consume and use that information nonetheless have a business need to	

access the location. This covers the risk while keeping the burden minimal. A more sustainable objective would be to ensure that all personnel with access are authorized rather than a strict need to know standard. Strict need to know implies compartmentalization that is not sustainable for large organizations with the need to deploy technicians across multiple districts. The language proposed so far would be sustainable if all information were stored electronically and cryptographically protected but this proposes a problem for hard copies stored in substations.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the qualifying language “with ERC” dropping from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligatations in the CIP Standards.

Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI). This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a sufficient protection.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST sees no benefit in moving BCSI storage location access management requirements from CIP-004 to CIP-011, and believes there is no need for clarification between BCSI and BCS requirements. Furthermore, N&ST believes that the impact of moving some access management requirements

from CIP-004 to CIP-011 could be significant for some Responsible Entities, compelling needless modification and disruption of mature and effective CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

Tri-State is generally ok with the movement of the requirements from CIP-004 to CIP-011. However, we do not agree with several of the changes.

1) We do not agree with the addition of PCAs to the scope. Furthermore, this was not in scope of the SAR to address.

2) As for R1.2, we think the original language was correct and the concept of “obtain and use” should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don’t recommend using the term “use” without providing more clarification as to its meaning.

3) Also as it relates to R1.2, we do not agree with the addition of “disposal”. While this is certainly a good security practice, adding this as a compliance requirement would be overly burdensome and unnecessary. Furthermore, this was not in scope of the SAR to address.

4) We think the modifications made to R3 are more prescriptive than the prior version in how to prevent unauthorized retrieval of BCSI and unnecessarily limits the entity’s options in how to meet the security objective. This should be reverted back to previous objective-based language. Furthermore, this was not in scope of the SAR to address.

Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information	
Likes 0	
Dislikes 0	
Response	
Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that meeting this objective likely requires minimal effort, AZPS recommends the SDT address the concept of designated storage locations throughout the Standard. Part 1.1 requires the identification of BCSI storage locations; however, subsequent Requirements omit references to storage locations and instead refer only to the protection of BCSI. The switch from storage locations to BCSI causes confusion and may create challenges in executing the required access management and protection controls.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	

CIP-004 is the appropriate place to require applicable levels of approval prior to granting access to BCSI. Removing the language from CIP-004 and adding it to CIP-011 creates two separate standards that cover access controls in place to protect the Bulk Electic System Information. CIP-011 defines what consititues BCSI and the requirements to protect it. It should not be an standard for approval, auditing and access monitoring.

Secondly, entities will be required to make major changes to their internal governance and compliance program procedures, policies and documentation in order to meet this requirement. Please do not mix standards/requirements

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The change made to CIP-011-3 Part 1.2 does not add clarity. The choice of the second “use” in Part 1.2 is confusing and does not make sense; “…by eliminating the ability to obtain and use BES Cyber System Information during, storage, transit, use, and disposal.” The SDT needs to elaborate on “…eliminating the ability…” What constitutes elimination of ability?

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

SMEC also disagrees with the removal of the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1, and how this greatly and needlessly expands the scope of all subsequent parts of R1, and R2

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

GSOC appreciates the SDT's consideration of the important concept of backwards compatibility; however, giving due consideration to the proposed scope expansion to include PCAs; the shift from access authorization to BCSI generally and not storage locations; the shift from methods to processes; and the incorporation of vendor risk assessments and required mitigations into the proposed requirements, GSOC cannot agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements.

Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

No, not as proposed.

There is a difference between authorizing access and provisioning access. Per CIP-004-6 Rationale for Requirement R4:

"Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6.

"Provisioning" should be considered the actions to provide access to an individual.

The scope of CIP-004 could be maintained while also changing the focus to the BCSI itself to meet the goals of the SAR by slightly modifying CIP-004 applicable requirement parts to "access to BES Cyber System Information in designated storage locations", such as in part 4.1.3:

R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.3 Access to BES Cyber System Information in designated storage locations.

CIP-004 R4.4 and R5.3 refer to **provisioned access**, and could be modified to include this language as well. For example:

R4.4 Verify at least once every 15 calendar months that provisioned access to BES Cyber System Information in designated storage locations is authorized and implemented correctly.

R5.3 For termination actions, revoke the individual's provisioned access to BES Cyber System Information in designated storage locations by the end of the next calendar day following the effective date of the termination action.

Likes 0	
Dislikes 0	

Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA appreciates the SDT's consideration of the important concept of backwards compatibility; however, giving due consideration to the proposed scope expansion to include PCAs; the shift from access authorization to BCSI generally and not storage locations; the shift from methods to processes; and the incorporation of vendor risk assessments and required mitigations into the proposed requirements, NRECA does not agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
While AEP is appreciative of the SDT's efforts to consolidate BCSI requirements into CIP-011, we do not feel there is minimal effort involved in ensuring compliance. Moving these requirements to a different standard creates more challenges that those who are responsible for complying are required to overcome, leading to more overall work and effort for those involved.	
Likes 0	

Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Black Hills would be in favor of seeing less perscriptive models of access and termination requirements. Additionally, the failure to remove BCSI per CIP-011 could potentially create a scenario where CIP-004's requirements were also unmet, creating a double violation.	
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 removal of the term "designated" greatly expands the scope to cover handling BCSI, including creating replicated copies of applicable BCSI, and ensuring applicable processes and controls are applied to new identified locations / instances of BSCI.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State is generally ok with the movement of the requirements from CIP-004 to CIP-011. However, we do not agree with several of the changes. 1) Tri-State does not agree with the addition of PCAs to the scope. Furthermore, this was not in scope of the SAR to address. 2) As for R1.2, we think the original language was correct and the concept of "obtain and use" should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to	

obtain and use it, which would align with the ERO Practice Guide. Although, we don't recommend using the term "use" without providing more clarification as to its meaning.

3) Also as it relates to R1.2, we do not agree with the addition of "disposal". While this is certainly a good security practice, adding this as a compliance requirement would be overly burdensome and unnecessary. Furthermore, this was not in scope of the SAR to address.

4) We think the modifications made to R3 are more prescriptive than the prior version in how to prevent unauthorized retrieval of BCSI and unnecessarily limits the entity's options in how to meet the security objective. This should be reverted back to previous objective-based language. Furthermore, this was not in scope of the SAR to address.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle finds the proposed requirements are not backward compatible in that they significantly expand scope, from controls for access to BCSI about High and Medium-with-ERC BCS, to access to all High and Medium BCS. Although this change does address the conflict between the different BCSI applicabilities of CIP-004 and CIP-011, it does not seem necessary to address the objective of the SAR, which is to revise the Standards to clearly accommodate BCSI storage and use solutions that are not based on local, physically-focused concepts. Like the change proposed in Q1 above, it is a clarifying change but appears to do little or nothing to address the central object of these revisions.

If specific access controls are deemed desirable, Seattle recommends that the access termination requirement be changed from the unique-to-BCSI "one calendar day" to the "24 hours" that is used for all other access termination requirements.

Seattle also supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3 since it

causes unnessessay revisions of the exsiting CIP-004 and CIP-011 progroms without gaining any

security values. CIP-004 were originally developed for centralizing the access management within one standard and we don't think SDT wants backwards, otherwise, does electronic access and physical access need to be moved back to CIP-004 to CIP-007 and CIP-006 as well?	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Disagree that the qualifying language “with ERC” was dropped from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3. This deletion greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself.

Lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as any such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. These Cyber Systems can only be compromised by breaching physical security, in which case this standard provides no protection.

There also is significant scope expansion with the authorization/revocation and review requirements now applying to all BCSI (not just designated storage locations of BCSI).

We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3. We appreciate the attempt to streamline Requirements associated with BCSI by placing all related compliance activities solely within the CIP-011-3 Standard. However, by doing so Responsible Entities would be subject to the potential of having multiple compliance issues with one failed compliance activity as a result of the overlapping NERC CIP Standards.

For example, it is conceivable that one process could remove the ability to access BCSI as well as other logical access. In this approach if there was a failure in this process it could result in a violation of both CIP-004-7 R5 and for CIP-011-3 R1, where under current Standards this situation would result in a single potential non-compliance with CIP-004-6 R5.

Due to these reasons we suggest that access control Requirements remain in CIP-004-6 with other access control Requirements.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The new standard expands the scope of BES CSI repositories to anywhere BES CSI may be, including in use and transit. This language is similar to the v3 language that was changed based on lessons learned. This may put entities across North America out of compliance because the current standard focuses on storage locations, not information in use or transit. Tracking BES CSI in use and transit will not be technically feasible and will but a great burden on business processes.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	
Comment	
Due to having a strong disagreement with R1.2, 1.4 and R2, we disagree with this clarity statement.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
While this change is minimal, it is relocated from the standard that contains all other authorization and provisioning requirements. This component of the requirement is about authorization, and is appropriate to be tracked and enforced in the same set of requirements, rather than potentially creating two separate violations when one violation would have occurred previously.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
The requirment in CIP-011-3 R1.2 appears circular. Are we trying to elimiate the abiltiy to use the BCSI while we are using it? System Information by eliminating the ability to obtain and **use** BES Cyber System Information during, including storage, transit, **use**, and disposal .	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the placement of access authorization and revocation as written in CIP-011-3, R1, Parts 1.3 and 1.5 does maintain backward compatibility to existing CIP-004 processes if an entity elects to use those existing processes. As noted in Question 1, PGAE does not agree storage locations need to be identified to establish the protections for the BCSI.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT agrees that the concepts of the current version of CIP-004 are maintained. However, a better approach may be to correct this with new parts in CIP-004. ERCOT also refers the drafting team to the comments submitted by ERCOT in response to Question No. 10.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	

Answer	Yes
Document Name	
Comment	
We agree that the concepts of the current version of CIP-004 are maintained. However, a better approach would be to correct this with new parts in CIP-004. Also see comments on question 10.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided 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 NextEra	
Answer	Yes
Document Name	
Comment	
1. We agree this update is backward compatible and this update provides greater flexibility.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
We agree this update is backward compatible and this update provides greater flexibility.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with moving the requirement to CIP-011. However, notes the change in applicabiltiy will be more than miminal effort to meet the new objectives.	
Likes 0	
Dislikes 0	
Response	
Calvin Wheatley - Wabash Valley Power Association - 1,3 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
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	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	

Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

3. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
I cannot find these references in CIP-004-7. If you are referring to CIP-011-3, we see where you are trying to go, but we dont think that it is clear enough.	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
The requirement mixes two types of usage needs. One is cloud storage and a separate requirement for vendors using information to perform work. The standard is appropriate for cloud storage type vendors. However, vendors using information for contract work should be moved or added to CIP-013 as part of an appropriate risk assessment.	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
There are too many ambiquities and additional clarity is required.	
Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment
The increase in storage solutions adds ambiguity this could have been done in a more effective way by removing references to physical and electronic storage. If this new version is intended to allow Storage as a Service model by external vendors, it should be clearified. We recommend that the BES CSI also be clearified to define terms such as 'context'.

Likes 0	
Dislikes 0	

Response
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment
Cloud storage and encryption technologies are not excluded under the current standards. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests that CIP-004-6 and CIP-011-2 already accommodate BCSI on the cloud. We believe it would be better to focus efforts on Requirements that do not hinder the use of other solutions while allowing for the development of access control programs by Responsible Entities that address risk posed to the industry. Any new Requirements need to meet the objective of protecting access to BCSI without constraining or prescribing types of storage solutions.

Likes 0	
Dislikes 0	

Response
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with the requirement language for achieving the SDT's goal. One of the SAR goals is to clarify the protections expected when utilizing third-party solutions (e.g., cloud services), but we haven't see the cloud storage and encryption language in the revised requirements yet.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
The revision succeeds in part but at the risk of considerable new ambiguities and unintended consequences (such as returning to the difficulty inherent in CIP v1-3 of controlling access to each individual piece of BCSI, or the necessity to understand the capability of an outside party to reasonably assess	

if they can “obtain and use” BCSI). The proposed language from CIP-011 R1.1 to R1.3 seems to Seattle a promising start to an objective-based, risk-focused approach to protection of BCSI, but then subsequent sub-requirements and requirements revert to an old-school prescriptive approach that creates confusion, speaks to specific technologies, and limits options. Seattle would prefer that a new Standard state a security objective, require a risk-based plan to meet this object (with certain, minimal components that must be in the plan), and then require implementation and periodic review of the plan.

Seattle also supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree that this approach is aproppriately reflected in the proposed requirements. Some items allow for expanded use of BCSI solutions; however, the new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance. Instead, these requirements should be objective based, which can be tailored to the specific solution and security options.

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 proposed language is too prescriptive and loses the focus on controlling access to BCSI. In its present form, it precludes technical advances that may improve how an RE controls access (e.g., geolocation, biometric, and other potential solutions).

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	
Comment	
Black Hills agrees that these changes make, what was understood to be possible under the current standards more explicit, however we are concerned that the standard remains too rigid. Instead we would prefer to see guidelines which then allow the RE to document its approach for using new technologies.	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	
Comment	
NRECA agrees that this is reflected in the proposed revisions; however, we are concerned that the way this has been incorporated places additional unnecessary compliance obligations on those entities that have chosen not to engage in the storage of BCSI in a cloud or other storage solution. Additionally, NRECA notes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions. For these reasons, NRECA is concerned that the proposed revisions will only work for specifically configured storage solutions and will not be properly scoped or flexible enough to accommodate the evolving storage and other solutions that could be employed in the future.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
Agree with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that this is reflected in the proposed revisions; however, is concerned that the manner in which this has been incorporated places additional unnecessary compliance obligations on those entities that have chosen not to engage in the storage of BCSI in a cloud or other storage solution. Additionally, GSOC notes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions. Finally, GSOC respectfully asserts that standard revisions to accommodate cloud storage are unnecessary and would be better addressed in implementation or compliance guidance. For these reasons, GSOC is concerned that the proposed revisions will only work for specifically configured storage solutions and will not be properly scoped or flexible to enough to accommodate the evolving storage and other solutions that could be employed in the future.	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Yes, agree that a stand alone requirement where a vendor stores an entitiy's BCSI is needed. 1.4.1 requires an initial risk assessment of vendors but the SDT needs to define what is acceptable evidence for a risk assessment.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
It is unclear in this draft or guidance how the SDT is expanding information storage soluctions or security technologies.	
Likes 0	
Dislikes 0	
Response	
Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that the SDT's intent is reflected in Part 1.4, the requirements as written do not clearly reflect an approach to expand information storage solutions or security technologies.	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T does not agree that this approach is apropppriately reflected in the proposed requirements. Some items allow for expanded use of BCSI solutions however, the new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance. Instead, these requirements should be objective based, which can be tailored to the specific solution and security options.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments.	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
While N&ST understands one of the SDT's key goals is to facilitate the use of an expanded array of storage options, we believe the associated imposition of a specific technology (encryption + key management) is likely to inhibit, not promote, the use of newer storage options such as cloud-based solutions. Furthermore, N&ST is concerned that the SDT's proposed changes could have significant cost and effort impacts on Responsible Entities that neither store BCSI in the cloud today nor have any plans to do so in the future.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We disagree because cloud based storage technologies and encryption technologies are not excluded under the current standards. The ERO Enterprise CMEP Practice Guide stated: BES Cyber System Information dated April 26, 2019 suggests that CIP-004-6 and CIP-011-2 already accommodates BCSI on the cloud.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

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

The question asks if the approach expands two different things: information storage solutions and security technologies. We agree the changes could allow for expanded storage solutions, but we do not agree that this approach expands security technologies for Responsible Entities. An example of a

security technology may be a cloud service that needs to use the information in order to provide security or reliability benefit to the BES. We find an applicable phrase in the “Industry Need” section of the SAR that states the expected reliability benefit is “providing a secure path towards utilization of modern third-party data storage **and analysis** systems” and the current draft doesn’t address third party analysis of the data to provide services to entities and actually further restricts such analysis.

It seems the approach is focused solely on using cloud storage for BCSI in an encrypted form and managing the encryption keys. Therefore, the focus seems to be on cloud **storage** only, not cloud **services** that need to use or analyze the data to provide services such as security monitoring technologies.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	
Comment	

We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019.

We agree with EEI comments that requirements should neither constrain nor prescribe solutions.

Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	
Comment	

We appreciate the SDT's effort to expand information storage solutions and security technologies; however, key management is the only technology that is explicitly detailed within the requirements. We feel that this is contradictory to what the 2016-02 SDT is working to accomplish with risk-based standards. Additionally, as the requirement is currently written, an entity would need to prove a negative if this requirement is not applicable to them, which is administratively burdensome. Finally, while it might not have been the SDT's intent, an auditor might interpret the requirement to mean that if an entity uses encryption internally (not with a third-party), then that entity must have a key management program, based on the requirement, for their internal encryption.

Likes 0	

Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO’s response assumes this question pertains to all proposed changes in CIP-011, requirement R1 (parts 1.1 – 1.5). The proposed changes as written, do not clearly draw out / articulate key distinctions that were noted during the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020: physical or electronic, responsible entity or vendor hosted. To make this clear in the proposed standard, MISO proposes the SDT include the following changes.	

Part 1.1. Modify the last example provided under Measures to read as follows: “Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity’s information protection program.”

Part 1.2 For clarity, modify the bullet under Measures as follows: “Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information, [delete the word "and"] key management program, retention in the Physical Security Perimeter).”

Part 1.3 May not be necessary if the SDT accepts MISO’s proposal to retain all access management provisions (BCS and BCSI) as part of CIP-004-7.

Part 1.4 MISO recommends the provisions in this section be eliminated from CIP-011-3 and addressed as part of CIP-013-2 thereby covering all vendor requirements (BCS and BCSI) in the same standard.

Part 1.5 MISO recommends the provisions in this section be eliminated from CIP-011-3 and addressed as part of CIP-004-7, requirement R5.3 thereby covering all access management requirements (BCS and BCSI) in the same standard.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

No, this approach is not clearly reflected in the proposed requirements. If the SDT’s intent is to provide direction on protection of BCSI stored in the cloud, it should be clearly stated by saying that these requirements are intended to address vendor operated storage locations or services. The vague language of “in cases where vendors store Responsible Entity’s BES Cyber System Information” opens a broad potential for auditor interpretation with unintended applicability, including instances where data has been shared with a vendor, but the vendor is not operating a storage location, or where a corporate resource with cloud functions is used to store working copies of data but is not a designated storage location.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI appreciates the SDT efforts to expand information storage solutions or security technologies for responsible entities. However, the proposed approach appears to be too prescriptive and inconsistent with elements of a results-based standard. The SDT should also ensure that the requirements are not tailored to any one solution or technology.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO's response is based on the assumption this question pertains to all proposed changes in CIP-011, requirement R1 (all subsections).

NYISO feels that the proposed changes do not clearly draw out or articulate key distinctions that were presented within the Q&A portion of the 2019-02: BES Cyber System Information Access Management Webinar hosted on January 16, 2020. NYISO feels that additional language be inserted to account for use cases (physical or electronic data being housed within either the responsible entity's controlled data centers or instances where the responsible entity has chosen to use vendor-hosted storage.

To make this clearer, NYISO proposes the SDT include the following changes:

Within Part 1.1: Modifications be made to the last example provided under Measures to read:

"Storage locations (physical or electronic, responsible entity or vendor hosted) be identified as housing BES Cyber System Information in the entity's information protection program."

Within Part 1.2: For clarity, modify the bullet under Measures to read:

"Evidence of methods used to prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information with a sound key management program, retention within the responsible entity's Physical Security Perimeter)."

NYISO feels that Part 1.3 will become unnecessary if the SDT retains all access management provisions (BCS and BCSI) within CIP-004-7.

NYISO would recommend that provisions contained in the current draft within Part 1.4 be removed from CIP-011-3 and addressed as part of CIP-013-2. This would have the effect of keeping all vendor requirements (BCS and BCSI) within the same standard.

NYISO would recommend that the provisions contained in the current draft within Part 1.5 be removed from CIP-011-3 and addressed as part of CIP-004-7. This would have the effect of keeping all access management requirements (BCS and BCSI) within the same standard.

Overall, NYISO would like to see all of the requirements in R1 be made clearer to allow the Responsible Entity latitude to choose any applicable security technologies that adequately protects BCSI, based on risk. Within the current draft, the language within R2 suggests that key management programs are mandatory; however, NYISO believes the intent was to allow other methods of protections as supported options.

Likes 0	
Dislikes 0	

Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
We believe the existing standard already allows multiple solutions. Why won't NERC/FERC tell Entities that the standard does not limited the scope of solutions available to entities and be done with this?	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
No, SNPD does not believe the SDT's objective has been met. SNPD believes that without explicit, affirmative authorization to use managed service ("cloud") storage solutions, Entities cannot and likely will not feel confident storing BCSI in the cloud. Entities will likely take the most conservative response to avoid potential compliance risk and simply choose not to use cloud storage solutions. Thereby, maintaining the status quo and depriving Entities of the flexibility desired under the proposed change. Suggestion: establish "reciprocity" from current Federal IT certification standards such as FedRAMP/FISMA/DoD D-ITAR. Issue a blanket statement that storage of BCSI is authorized in any/all FedRAMP/FISMA or DoD D-ITAR cloud. This type of verbiage is both actionable and clear.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	

While Alliant Energy appreciates the SDT's efforts to expand information storage solutions or security technologies for responsible entities, that expansion is only useful if the requirement language is written such that it is clearly auditable. The updated requirements should avoid the ability to audit to prescriptive requirements that are not stated in the language of the requirements.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	

Comment

See Steven Toosevich's comments.

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

There is no expansion of solutions or technologies used. The proposed requirements codify the controls that have been discussed in informal manners. This is a slight improvement, but as long as CIP requirements can also be interpreted as applicable for cloud vendors and are in the audit scope of CIP audits, there is no real improvement.

Recommend excluding cloud vendors from applicability column of BCSI requirements and, instead setting requirements to be included in risk assessments of cloud vendors and have the CIP senior manager or delegate approve each assessment and applicable risk mitigations at minimum intervals. In addition cloud vendor requirements appears to be better addressed through CIP-013.

BCSI related cloud vendor risk assessment components can be a subset of CIP004 or CIP011 requirements that meet cloud vendor industry best practices such as the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) and the provision of certifications (e.g. ISO 27000) or audit reports (e.g. SOC for security) from accredited auditors who have verified cloud vendor claims of compliance.

Likes 0	

Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
No, in order to provide expanded security technology solutions (read "in the cloud"), the vendor may need both access and use of BCSI to provide any value to the registered entity. The approach offered in this proposal does not allow this access.	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
We believe the existing standard already allows multiple solutions. Why won't NERC/FERC tell Entities that the standard does not limited the scope of solutions available to entities and be done with this?	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019. We agree with EEI and MRO NSRF comments that requirements should neither constrain nor prescribe solutions.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
There is no expansion of solutions or technologies used. The proposed requirements codify the controls that have been discussed in informal manners. This is a slight improvement, but as long as CIP requirements can also be interpreted as applicable to cloud vendors, and are in the scope of CIP audits, there is no real improvement.	

ERCOT recommends excluding cloud vendors from the applicability column of BCSI requirements, and instead setting requirements to be included in risk assessments of cloud vendors and having CIP senior managers or delegates approve each assessment and applicable risk mitigations at minimum intervals. In addition, cloud vendor requirements appear to be better addressed through CIP-013.

BCSI related cloud vendor risk assessment components can be a subset of CIP-004 or CIP-011 requirements that meet cloud vendor industry best practices such as the Cloud Security Alliance (CSA), Consensus Assessments Initiative Questionnaire (CAIQ), and the provision of certifications (e.g. ISO 27000) or audit reports (e.g. SOC for security) from accredited auditors who have verified cloud vendor claims of compliance.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We disagree with the proposed approach, as we do not see the necessity. Cloud-based storage technologies and encryption technologies are not excluded either under the current standards, or by the ERO Enterprise CMEP Practice Guide BES Cyber System Information dated April 26, 2019.

We agree with EEI and MRO NSRF comments that requirements should neither constrain nor prescribe solutions.

Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
There has to be a better definition of the different storage and security technologies the SDT is considering. There will be a big difference between on premise and external solutions.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: While there is clearly an effort to address expanded use of information storage solutions and security technologies, the current draft does not specifically address use cases associated with cloud services and information sharing with external parties as clearly as will be required. For entities to make use of options available from external service providers, there will need to be specification of information protections specific to such situations (i.e. whether individual access to information must be demonstrated by the service provider to the responsible entity and the expectations for measures to demonstrate compliance of a third party).	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

SunPower agrees with MRO NSRF's comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: Although the language allows Entities to expand information storage solutions, it then leaves the Entity open to risk due to interpretation of how their process and security measures are interpreted by an auditor. As long as there is consistency in audit, that if an Entity follows their process, as required by the standard, no audit findings will be given. If an auditor takes issue with the Entity's process(es) or security technology, an audit recommendation would be given, not a finding and or associated fine.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees that this approach is reflected in the proposed requirements. However, the requirements as written are problematic for reasons provided in subsequent responses.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP is of the opinion that the approach to expand information storage solutions is reflected in the proposed modifications. However, we feel that while this approach may help organizations having information storage isssues, we also feel that this approach produces security concerns as a result of BCSI being stored using cloud technology.	
Likes 0	
Dislikes 0	

Response
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations
Answer Yes
Document Name
Comment
Although the language allows Entities to expand information storage solutions, it then leaves the Entity open to risk due to interpretation of how their process and security measures are interpreted by an auditor. As long as there is consistency in audit, that if an Entity follows their process, as required by the standard, no audit findings will be given. If an auditor takes issue with the Entity's process(es) or security technology, an audit recommendation would be given, not a finding and or associated fine.
Likes 0
Dislikes 0

Response
Leonard Kula - Independent Electricity System Operator - 2
Answer Yes
Document Name
Comment
No comment.
Likes 0
Dislikes 0

Response
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5
Answer Yes
Document Name
Comment
Yes the expanded approach is available in the proposed standard; however, as discussed later, the requirements need to be improved.
Likes 0
Dislikes 0

Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PGAE believes the modifications expand the capability to use third-party service providers without a risk of being non-compliant based on different interpretations of the current Standards. The method(s) or technology used to protect the BCSI are non-prescriptive, providing the necessary flexibility to meet the objective of preventing unauthorized access.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 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	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
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 NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

4. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

1.2 becomes extremely burdensome by eliminating the ability to obtain and use BCSI during storage, transit, use, and disposal. Entities may need to employ methods such as chain of custody for disposal of hard drives that may contain BCSI.

SunPower encourages the term “reduce” the ability to obtain and use BES Cyber System Information during storage, transit, use. . .

Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments:

The inclusion of the terms “obtain and use” help to more accurately identify the objective of the access protections that need to be implemented. However, inclusion of those terms does not accurately address the risk related to the potential compromise of BCSI.

Moreover, the term “eliminating” is an absolute, so implementation and compliance would be challenging to demonstrate.

Recommendation: change the language to “methods to prevent the ability to obtain and use BCSI information through unauthorized access including storage, transit, use and disposal.”

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The previous Part 1.2 approach gave Responsible Entities flexibility to accurately address the risk related to the potential compromise of BCSI. The new Part 1.2 approach does not appear to give Responsible Entities thae same flexibility, especially if third-party solutions (e.g., cloud services) are not utilized. If the purpose of the new Part 1.2 approach is to address the risk associated with the use of a third-party solution (e.g. cloud services), the Part 1.2 requirement language should be made more clear than is currently proposed. IPC requests that the SDT provide additional rationale information related to “the ability to obtain and use BES Cyber System Information” language in the proposed requirement as it is unclear what is intended by the phrase “obtain and use” in the requirement. IPC believes the Part 1.2 requirement language should focus more on a Responsible Entity ensuring they have appropriate measures in place within their BES Cyber System Information (BCSI) Protection Program to protect BCSI rather than requiring entities to encrypt their data in transit, storage, and use.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	

Comment
Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.” The draft R1 Part 1.2 Requirement could then be revised to “Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use.” We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.” We concur with MRO NSRF comments that disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection. Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

The draft R1 Part 1.2 Requirement could then be revised to “Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use.”

We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.”

We concur with MRO NSRF comments that disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1

Answer	No
Document Name	

Comment

Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike

Answer	No
Document Name	

Comment

There appears to be a significant challenge with the proposed wording of Requirement Part 1.2, which appears to require entities to eliminate the ability to obtain and use BCSI even for authorized access holders.

Suggest the following replacement requirement text:

"Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability of unauthorized users to obtain and use BES Cyber System Information during storage, transit, use, and disposal."

OR

"Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal, to authorized access holders."

While this approach is better than previous approaches, there is still a need for security technology vendor service providers to have access and use of BCSI. The proposed update does nothing to allow MSSPs in a CIP program. Along with allowing Authorized users to both obtain and use, the EACMS split to EACS and EAMS is also required to allow MSSPs.

Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI’s comments	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	

Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD does not agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach and verbiage. However, SNPD supports the reasoning behind the proposed change.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro requests more clarity as to what is the extent of the application of the term “elimination” that is now included in the requirement. Please add clarity within the language of standard. Example: Is an encryption key sufficient to “eliminate” even though this is potentially hackable? BC Hydro would also request additional clarity on what the “ability to use BCSI” means.	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI has concerns with defining risks regarding potential compromise of BCSI within the language of a Reliability Standard. EEI suggests that it may be simpler to address BCSI security concerns through the development of a definition for “Useable Access” within the NERC Glossary of Terms. We also suggest the SDT consider using the language from the April 26, 2019, ERO Enterprise CMEP Practice Guide on BES Cyber System Information which	

appears to have the requisite clarity and could act as a clear definition for “Useable Access” (see below). If the term is deemed to be unsuitable, the SDT could use the phrase “Access to the BCSI….”

Useable Access: An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access. Ref.: Page 2, Bullet 1: https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

In consideration of access, CIP-004-6 already effectively addresses access controls for BCSI when stored by responsible entities at their facilities so protections would only need to be developed for a situation where third party cloud-based services are used. Consequently, the above reference *CMEP Practice Guide* could effectively define access in a manner that addresses this issue.

Within this alternative approach and once the definition for “Useable Access” is addressed, the changes needed to meet the intent of the SAR could be simply accomplished through the following changes to CIP-004-6:

4.1.1. Electronic Access

4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.1.3. Useable Access to a BCSI Repository

The SDT should also consider restoring the language of CIP-004-6 R5.3, with the modification as shown below, or something similar, that achieves a similar result:

*For termination actions, revoke the individual’s **Useable Access** to **a BCSI Repository**, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.*

With the proposed solution, the language within CIP-004-6, Part 5.3 could be largely retained while limiting the scope of any vendor’s “Useable Access.” In such a situation, the vendor is simply a custodian to encrypted or otherwise masked data and does not have the ability to use it. Additionally, vendors with “Useable Access” (i.e., both custody of data and ability to use BCSI) would continue to need provisional access granted by the responsible entity through their established access control process and procedures.

Lastly, EEI is concerned with the compliance issues in using the term “eliminate” as proposed in CIP-011-3 R1.2. The word “eliminate” is ambiguous when considered within the context of demonstrating compliance. It will be difficult to prove to an auditor that the responsible entity has eliminated all risk. EEI suggests that the SDT modify the language and replace “eliminate” with “limit” or some similar language.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE recommends using the words “or” instead of “and” and proposes the following alternative:

"Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain or use BES Cyber System Information during storage, transit, use, and disposal."

Protections to prevent access, like access control to the storage location, are separate and distinct from controls to prevent use, like encryption during transit. Entities may have systems with one but not the other, if the system is all in house and physically protected. The proposed language would not be backward compatible.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment
While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording. One of the below listed changes should be made to these modified Standards. We recommend changing Part 1.2 from <<Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>> To <<Method(s) to prevent the ability to obtain and use BES Cyber System Information through unauthorized access during, including storage, transit, use, and disposal.>> because “eliminating” is an absolute which makes implementation and demonstrating Compliance too challenging.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	

Comment
Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI

and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access."

The draft R1 Part 1.2 Requirement could then be revised to "Method(s) to prevent unauthorized BCSI Access during BCSI storage, transit, and use."

We disagree with the phrase, "by eliminating the ability" to obtain and use. This represents an unachievable threshold over and above the current "Procedure(s) for protecting and securely handling."

We concur with MRO NSRF comments that disagree with the addition of "and disposal" to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements "that contain BES Cyber System Information." Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the Measures would need to address examples of acceptable evidence of disposal, such as shredding for paper. We do not see a practical method of evidencing the disposal of electronic BCSI, i.e. the day-to-day deletion of electronic files.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The language of "eliminating the ability to obtain the and use BES Cyber Information" sounds ambiguous. Also, the term "use" that occurs twice within a sentence need more clarification.	
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	

We do not agree with the modifications to Part 1.2 for the following reasons:

- It requires methods to "prevent" unauthorized access. We caution against using "100% words" in situations such as this because if ever a piece of encrypted information is cracked, the entity's method did not 100% prevent it. A technology breakthrough or suddenly discovered vulnerability in an encryption algorithm that enables cracking today's encryption protocols makes the entire industry suddenly non-compliant.

- R1.2 goes on to say the process must prevent unauthorized access BY eliminating the ability to obtain and use BCSI. A literal reading of this requirement says that entities must prevent unauthorized access by eliminating ALL ability for anyone to obtain and use BCSI. We understand this phrasing is attempting to define "access", but the way this is stated it says you must prevent unauthorized access by eliminating all access.

- Adding “disposal” to R1.2 is duplicative of R3. That’s now required twice in two different requirements within the same standard, and we do not support including it here. We also question how “disposal” of BCSI is not inherently included in “storage, transit, and use” and why the additional qualifier is needed?

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA understands “obtain” to mean take possession of, and “use” to mean take an action on. “Obtain” is not much clearer than “gain access to” while “use” does add an element of clarity to the objective of what needs to be protected. “Use” implies that obtaining “unusable” (i.e., encrypted) information is a lesser risk.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with using the terms “obtain” and “use”. However, this will require the Responsible Entity document what the the terms “obtain” and “use” mean with respect to BCSI – we believe more explanation is needed within the requirement or guidelines.

Based on the CMEP BCSI practice guide. The practice guide provides very little additional information on what is meant by “obtain” and “use.” Without additional guidance evidencing this concept for audit purposes (that someone obtained BCSI but couldn’t use it) would be a significant challenge.

We disagree with the phrase, “by eliminating the ability” to obtain and use. This represents an unachievable threshold over and above the current “Procedure(s) for protecting and securely handling.”

Likes 0	
Dislikes 0	

Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST does not believe the proposed terms will enhance general understanding of the risks associated with potential compromises of BCSI. In N&ST's opinion, the NERC Glossary definition of BCSI ("Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.") more than adequately defines the potential risks. Furthermore, in recent discussions with representatives from several Responsible Entities, it has become apparent to N&ST that there is NO good consensus on what it means to "use" BCSI. We believe the existing language in CIP-011-2, Requirement R1 Part 1.2 should be retained.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments. For key retention in R1.2 of CIP-011, is this saying that where the key is stored needs to be behind a PSP?	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T does not agree. Clarity is needed around what "use" means, especially considering this is an issue that currently exists under the version that is in effect. Similarly, there would need to be more clarity around the meaning of the term "obtain".	

As for R1.2, we think the original language (other than “use” not being defined) was correct and the concept of “obtain and use” should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don’t recommend using the actual terms “use” and “obtain”, without providing more clarification as to their meaning.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

The intention is good; however, the current proposed requirement language does not accomplish that intention; instead it seems to completely preclude the use of BCSI the way it is written.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

While AZPS agrees that the inclusion of “obtain” and “use” more clearly addresses the risk related to the potential compromise of BCSI, AZPS believes that the proposed language in Part 1.2 creates an undue burden for Entities to execute and evidence “eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal”. AZPS recommends that the SDT retain focus of the requirement language on “protecting and securely handling” BCSI, and address the inclusion of “obtain” and “use” in guidance documents. AZPS offers proposed changes for Part 1.2 below:

“Procedure or method(s) to prevent unauthorized access, protect, and securely hande BES Cyber System Information during storage, transit, use, and disposal”.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
WAPA requests changing the work “use” in the last sentence of the requirement. “BES Cyber System Information during storage, transit, use and disposal.” To “BES Cyber System Information during storage, transit, and disposal. The lack of a clear definintion for the word “use” creates major problems for Registered Entities (REs). Use in context of BCSI displayed a system screen, BCSI layed out on a drafting table, BCSI posted in a response/job aid binder being read by an aoperator or BCSI in computer systems memory address? Without a better definition REs will need to implement procedures to address these scenarios; some of which are not commercially viable (memory encryption).	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The change made to CIP-011-3 Part 1.2 does not add clarity. The choice of the second “use” in Part 1.2 is confusing and does not make sense; “…by eliminating the ability to obtain and use BES Cyber System Information during, storage, transit, use, and disposal.” The standards drafting team needs to elaborate on “…eliminating the ability…” The SDT should remove the second “use”.	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
It is impossible to completely “prevent” and or “eliminate” the ability to obtain and or use BCSI during storage, transit, use, and disposal, so all Entities would be in violation the way this is written. The reasons the standards exist are to lower cyber security risks to the BPS. Suggest replacing “eliminating” with “reducing” or rewording the requirement language to: “Method(s) to reduce the risk of unauthorized access to BCSI during storage, transit, use and disposal.”	

Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the approach essentially “eliminates” the risk associated with use of BCSI as the revisions require entities to completely eliminate the ability to obtain or use BCSI during nearly all life stages with the exception of creation. GSOC respectfully suggests that use of the term “eliminate” was inadvertent and should be revised to “control” or “restrict.” Should the SDT remove the term “eliminate” and replace it with a feasible alternative, this requirement could achieve its intended purpose. However, GSOC also notes, for the SDT’s consideration, the infeasibility of the term “prevent.” Responsible Entities cannot “prevent” or “eliminate” every risk or capability that could possibly manifest during the life cycle of BCSI. Further, it is difficult to conceive of how prevention of “unauthorized access” would be documented and proven during compliance monitoring. For this reason, GSOC recommends that the SDT revise the requirement to indicate an affirmative obligation to manage or control access rather than an obligation to prevent access, which would effectively require Responsible Entities to “prove” that unauthorized access did not occur rather than proving that they “controlled” or “managed” access through proactive security controls. Such a revision will not only reduce the potential for confusion around whether unauthorized access was “prevented,” it will also remove the likelihood that Responsible Entities would be required to “prove a negative” during compliance monitoring activities. For these reasons, GSOC recommends that the SDT consider revising the requirement as proposed below. Method(s) to manage access to BES Cyber System Information during storage, transit, use, and disposal.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

While we appreciate the SDT's effort to clarify what access means, this is better left to guidance documents, like it is now in the CMEP Practice Guide: BES Cyber System Information, dated April 26, 2019. Without the additional context that the guidance document provides, this language just adds confusion to the requirement. In addition, the ability to *use* information is open to interpretation, such as whether or not the individual has the knowledge to use the information in such a way as to affect the BES.

Also, it is not possible to completely *eliminate* the ability to obtain and use BCSI, so "eliminate" should not be used.

Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA agrees that the approach essentially "eliminates" the risk associated with use of BCSI as the revisions require entities to completely eliminate the ability to obtain or use BCSI during nearly all life stages with the exception of creation. NRECA believes that use of the term "eliminate" was inadvertent and should be revised to "control" or "restrict." Should the SDT remove the term "eliminate" and replace it with a feasible alternative, this requirement could achieve its intended purpose. However, NRECA also notes, for the SDT's consideration, the infeasibility of the term "prevent." Responsible Entities cannot "prevent" or "eliminate" every risk or capability that could possibly manifest during the life cycle of BCSI. Further, it is difficult to conceive of how prevention of "unauthorized access" would be documented and proven during compliance monitoring.

For this reason, NRECA recommends that the SDT revise the requirement to indicate an affirmative obligation to manage or control access rather than an obligation to prevent access, which would effectively require Responsible Entities to "prove" that unauthorized access did not occur rather than proving that they "controlled" or "managed" access through proactive security controls. Such a revision will not only reduce the potential for confusion around whether unauthorized access was "prevented," it will also remove the likelihood that Responsible Entities would be required to "prove a negative" during compliance monitoring activities. For these reasons, NRECA recommends that the SDT consider revising the requirement as proposed below:

"Method(s) to "manage" access to BES Cyber System Information during storage, transit, use, and disposal."

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not believe that the new language being proposed effectively addresses risks associated the compromise of BCSI. AEP has no opinion on the inclusion of the words “obtain” and “use”, but the inclusion of the word “eliminating” is a cause for concern. The absolute nature of the word has brought about concerns that it would be difficult to prove compliance.	
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 removal of the word “designated” creates an insurmountable scope of program management. The use of the word “eliminate” sets an impossible threshold to achieve.	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
There are issues with the wording. "eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal"	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State does not agree. Need more clarity around what "use" means, especially considering this is an issue that currently exists under the version that is in effect. Similarly, there would need to be more clarity around the meaning of the term "obtain". As for R1.2, we think the original language (other than "use" not being defined) was correct and the concept of "obtain and use" should instead be incorporated into the access requirements, especially R1.3. This will make it clear that in order for someone to be deemed to have access to BCSI, they must have the ability to obtain and use it, which would align with the ERO Practice Guide. Although, we don't recommend using the actual terms "use" and "obtain", without providing more clarification as to their meaning.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Seattle supports the comments of SMUD to this question.	
Likes 0	
Dislikes 0	

Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Disagree with the phrase “by eliminating the ability to obtain and use” and it should be moved to Guidelines and Technical Basis to explain what constitute a BCSI access. Agree with adding disposal since it was missing from current CIP-011-2 R1.2. Suggest making the following changes for R1 Part 1.2: “Method(s) to prevent unauthorized access to BES Cyber System Information during, including storage, transit, use, and disposal.” Suggest adding the following language into Guidelines and Technical Basis based on CMEP BCSI Practice Guide: “BCSI access means any instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Agree with terms “obtain” and “use;” however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. Recommend defining “BCSI Access” in the NERC Glossary of Terms per the practice guide: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

Disagree and very concerned with the phrase “by eliminating the ability” to obtain and use. This represents an unachievable evidencing threshold over and above the current “Procedure(s) for protecting and securely handling.” Responsible Entities can document protective procedures, but will be hard pressed to prove they have eliminated all ability to obtain and use, i.e. rendered unauthorized access impossible.

Disagree with the addition of “and disposal” to the end of the requirement. BCSI in BES Cyber Systems is already addressed in R3 Part 3.1., but Part 3.1 needs to reinstate the qualifying language in the Requirements “that contain BES Cyber System Information.” Deletion of this qualifying language is an expansion of scope to the current CIP-011-2 R2 requiring evidence of sanitization of assets not containing BCSI subject to this protection.

Although a logical inclusion as part of the lifecycle of BCSI, as applied in R1 Part 1.2, the evidencing we do in R3 for hardware is now going to be extended to the disposal/deletion of BCSI, on every medium, wherever stored, since the Measure calls for “Evidence of methods used to prevent the unauthorized access…” during disposal. The evidencing burden here can be crushing. Example concerns include:

- How will auditors know what BCSI has been disposed of unless Entities maintain an active inventory of BCSI “info items” and status, active or disposed, just like we do for BES Cyber Systems?

- Entity may have a policy to shred paper-based BCSI as the disposal method, but to evidence the method was used, does Entity have to log documents shredded?

- Will every electronic file, document, or email containing BCSI require its deletion to be logged by IT? Will Entities have to obtain such logs from third-party vendors/data custodians?

Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The ‘obtain’ and ‘use’ terms are not defined and will lead to additional ambiguity and confusion. It is impossible for entities to know the capabilities of potential threats, ‘use’ from one party may be different than another.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

1. CIP-011 R1, Part 1.2 states “*….by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal*.” Does a format of portable storage media (e.g. flash drives) eliminate the ability to obtain and use BCSI?

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Adding the additional terms of “obtain” and “use” to try to imply the use of encryption without explicitly stating the requirement weakens the language. Further, the use of the word “eliminating” adds significant burden to entities to prove their choosen method can never be compromised. Removal of the phrase “by eliminating the ability to obtain and use BES Cyber System Information” makes the requirement clear and allows entities to select current

and future technologies to protect BCSI during storage, transit, use, and disposal. Consequently, by including these four phases protections for “obtaining” access and during “use” are included in a number of current storage and transit technologies.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy generally agrees that the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2 will more accurately address the risk related to the potential compromise of BCSI. Duke Energy foresees a challenge to be able to demonstrate how we “eliminate” the ability to “obtain and use” BCSI. Suggest change "eliminating" to "limiting" or "restricting". Insert "both" before "obtain and use".	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Comments: It is impossible to completely “prevent” and or “eliminate” the ability to obtain and or use BCSI during storage, transit, use, and disposal, so all Entities would be in violation the way this is written. The reasons the standards exist are to lower cyber security risks to the BPS. Suggest replacing “eliminating” with “reducing” or rewording the requirement language to: “Method(s) to reduce the risk of unauthorized access to BCSI during storage, transit, use and disposal.”	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
As long as both terms are defined properly, this methodology will help improve the storage of BCSI requirement.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the inclusion of the “obtain” and “use”. PG&E recommends that examples of what is “obtain” and “use” be included in the Technical Rationale document to help better understand the intended meaning and to avoid potential future interpretation differences or ambiguities.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT believes this is an improvement and provides clarity on the meaning of unauthorized access.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
However, see other Entities comments related to wording change suggestions	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
This is an improvement and provides clarity on the meaning of unauthorized access.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
However, see other Entities comments related to wording change suggestions.	
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 NextEra	
Answer	Yes
Document Name	
Comment	
While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording. We recommend changing Part 1.2 from <<Method(s) to prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>> To <<Method(s) to prevent the ability to obtain and use BES Cyber System Information through unauthorized access during, including storage, transit, use, and disposal.>> because “eliminating” is an absolute which makes implementation and demonstrating Compliance too challenging.	
Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	

Comment

NYISO feels that “Obtain” and “use” are key distinctions providing clarity related to what is required to prevent unauthorized access. NYISO would also suggest that the following modification be made to the Requirements language:

“Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to both obtain and use BES Cyber System Information during storage, transit, use, and disposal.” In the case where BCSI is encrypted, information could still be obtained (physically or electronically) but would not be in a usable format.

Note – During the Q&A session on the 2019-02: BES Cyber System Information Access Management *webinar (*January 16, 2020*), it appears that “access” equated to having the ability to “obtain and use.” Part 1.2 language seems to be focused on the prevention of unauthorized access by “restricting” the ability to “obtain and use,” NYISO recommends the SDT clarify this point within the Technical Rationale for Reliability Standard CIP-011-3.*

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	

Comment

Yes – somewhat. “Obtain” and “use” are key distinctions which help provide better clarity related to what is required to prevent unauthorized access. In addition, MISO suggests the following modification to the Requirements language:

“Method(s) to prevent unauthorized access to BES Cyber System Information by [delete the word "eliminating"] *restricting* the ability to *simultaneously* obtain and use BES Cyber System Information during storage, transit, use, and disposal.”

Note – based on the Q&A session during the 2019-02: BES Cyber System Information Access Management *webinar* hosted on January 16, 2020*, it appears that “access” equates to having the ability to “obtain and use.”*

As the intent of Part 1.2 is to prevent unauthorized access by “restricting” the ability to “obtain and use,” MISO recommends the SDT clarify this point in the Technical Rationale for Reliability Standard CIP-011-3.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

While we understand why “obtain and use” are included in Part 1.2, we fear that the way the requirement is written, the intent will be obscured. For instance, the word “eliminating”, implies perfect execution. This is unattainable and should be avoided in the requirement language. While the changes to this part are a good start, we feel that they are too narrowly focused on cloud-service providers and add extra burden to existing information protection programs.

We encourage the SDT to develop a thoughtful process across all of CIP-011.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

Yes the requirement is improved with the suggested terms "use" and obtain". However, the proposed requirement is somewhat circular and should be further improved as follows:

"Method(s) to prevent unauthorized access to BES Cyber System Information during storage, transit, use, sanitization, and disposal." (The inclusion of sanitization here eliminates the need for R3 Part 3.1.)

The term "eliminating" suggests a zero-defect approach, which is an extremely challenging compliance outcome to achieve.

The second bullet in the both R1 Part 1.2 and Part 1.3 Measures is fragmented and introduces topics (e.g. key management program) that have yet to be presented in the standard.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes

Document Name	

Comment

IESO agrees in principle with the comments submitted by NPCC:

While we agree that “obtain” and “use” more accurately address the risk, we have concerns with the overall wording because “eliminating” is an absolute (i.e. zero defect) which makes implementation and demonstrating Compliance too challenging

We recommend changing Part 1.2 from

<<Method(s) to prevent unauthorized access to BES Cyber System Information by *eliminating* the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal.>>

To

<<<<Method(s) to prevent unauthorized access to BES Cyber System Information by *controlling* the ability to obtain and use BES Cyber System Information during, including storage, transit, use, and disposal .>>

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

The ability to “obtain and use” allows for the use of encryption as an acceptable means of protecting BCSI and helps to clarify “knowing and utilizing the information” is what were aiming to protect, instead of simply possessing it. Additionally, Black Hills would like to see “Use” definded in the Glossary.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

If you can clean up the sentance better.

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach. This focus is on the BCSI (data) versus applicable systems that would contain BCSI. This also aligns with the CMEP Practice Guide: ERO Enterprise CMEP Practice Guide BES Cyber System Information. Texas RE does have a concern that entities could simply use the bare minimum controls. For example, a registered entity could comply using encryption, but there is no established brightline criteria indicating what level of encryption is sufficient to meet the objective of this requirement. This may result in inconsistent enforcement of this requirement across the regions. If encryption is to be considered an acceptable means of prevent unauthorized access to BES Cyber System Information then Texas RE recommends that the SDT review NIST Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, and incorporate guidance from the NIST publication into the CIP standard where appropriate and applicable. Additionally, in the measures an example of evidence is 'retention in the Physical Security Perimeter.' Texas RE agrees that for BCSI in a physical form retention in a PSP is an adequate means of protection. However, the PSP would not be considered adequate protection for electronic BCSI that is located on a server outside of the Entity's ESP.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

Due to strong disagreements with 1.2, 1.4 and R2, we disagree here.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We can agree with identifying BCSI in CIP-011-3 R1.1 and then using BCSI only in later applicability tables, but cannot support the removal of Medium Impact BES Cyber Systems with ERC.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	

Comment
Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	

Comment
Although Seattle finds the proposed approach intriguing, it also finds unnecessarily confusing the inconsistent application of this approach among R1.1-R1.3 and R1.4-1.5, R2, and R3. Better would be to revise the entire Standard one way or the other. Seattle also believes that an objective-based, risk-focused approach would eliminate the need to add “BCSI” to the Applicability column at all. It would be up the entity to specify its own controls in its plan and whether they are controls for BCSI about specific impact ratings of BCS, BCSI storage locations, third party BCSI storage providers, etc.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
While having BCSI in the applicability column provides clarity, it unfortunately expands the scope of the requirements beyond what they are today. If the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS.

We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

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

What was the intent of stating “BCSI as identified in R1.1”? Is the SDT inferring that other BCSI exists that was not identified in R1.1?

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Black Hills does not think the current definition of BCSI provided in the Glossary is clear enough to allow for BCSI to be listed as an *Applicable System*. We think it would make more sense to leave applicability listed as High and Medium BCS… and state in the requirement “For BCSI, perform action “X,”” as the current CIP-004 R4.1 is modeled, for example.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

While NRECA understands what the SDT was attempting to accomplish and does not disagree with the intended clarification, the replacement of "Applicable Systems" with "Applicability" is problematic as such term is already utilized in Section 4 of the CIP-011 standard, and, there, it is utilized to denote whether a registered function has responsibility under the Standard. Utilization of the same term, but with a different scope within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of CIP-011. Further, this change results in CIP-011 being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. Finally, NRECA notes that it is also concerned that the modifications to the contents of the "Applicability" column conflict with the definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the "applicability" to "system information pertaining to…" while BCSI is defined as

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

There is information that is not "system information pertaining to" a particular asset that could be used to "gain unauthorized access or pose a security threat to the BES Cyber System." Further, the definition makes explicit reference to "security procedures or security information;" neither of which is confined to "system information" and both of which may be comprised of information that is not "system information." These potential conflicts and contradictions between the standard and the Glossary of Terms Used in NERC Reliability Standards could result in increased ambiguity and confusion.

Finally, NRECA notes that requirement applicability is already complicated and in need of simplification. This modification and addition of the same term within the standard and requirement only serves to increase the complexity and the likelihood for ambiguity and confusion. As well, it must be noted that this change presents a substantial challenge to audit as the implication is that all system information must be evaluated to demonstrate that it was evaluated for identification as BCSI and, further, relative to compliance monitoring activities, all such system information must be available to sample to determine whether the process identified it as BCSI or not. NRECA does not agree that this provides better clarity on the focus of the requirements and, therefore, does not support this change.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

We disagree with changing the column heading and adding “system information pertaining to” for the following reasons. First, it is inconsistent with other standards and it is confusing to have “applicability” here and also in section A.4 where it lists “Applicability” of functional entities and facilities. Secondly, the definition of BCSI includes information about low impact systems. Therefore, we will be identifying all BCSI in our organization as required by R1 Part 1.1. However, the applicable systems column defines the scope of systems to which the requirement row applies. By referring to “BES Cyber System Information as identified in Requirement R1 Part 1.1” for the applicability of subsequent parts, the scope of systems to which the requirements applied has been increased, since we will have identified BCSI pertaining to low impact systems as well. Third, CIP-011 has always been about BCSI, regardless of where it is stored, so this does not clarify anything further.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

While GSOC understands what the SDT was attempting to accomplish and does not disagree with the intended clarification, the replacement of “Applicable Systems” with “Applicability” is problematic as such term is already utilized in Section 4 of the CIP-011 standard, and, there, is utilized to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of CIP-011. Further, this change results in CIP-011 being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. Finally, GSOC notes that it is also concerned that the modifications to the contents of the “Applicability” column conflict with the definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the “applicability” to “system information pertaining to…” while BCSI is defined as

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

There is information that is not “system information pertaining to” a particular asset that could be used to “gain unauthorized access or pose a security threat to the BES Cyber System.” Further, the definition makes explicit reference to “security procedures or security information;” neither of which is confined to “system information” and both of which may be comprised of information that is not “system information.” These potential conflicts and contradictions between the standard and the Glossary of Terms Used in NERC Reliability Standards could result in increased ambiguity and confusion.

Finally, GSOC notes that requirement applicability is already complicated and in need of simplification. This modification and addition of the same term within the standard and requirement only serves to increase the complexity and the likelihood for ambiguity and confusion. As well, it must be noted that this change presents a substantial challenge to audit as the implication is that all system information must be evaluated to demonstrate that it was evaluated for identification as BCSI and, further, relative to compliance monitoring activities, all such system information must be available to sample in

order to determine whether the process identified it as BCSI or not. For these reasons, GSOC does not agree that this provides better clarity on the focus of the requirements and, therefore, cannot support this change.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

R1.2 - No

R1.3 – Move to R1.5 - these specific requirements should be placed in the appropriate standards CIP-004 and CIP-013.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

AZPS does not agree that the proposed revisions to the “Applicability” column provides better clarity on the focus of the requirements. AZPS requests revising the applicability column to read as follows: “System information pertaining to (but not including the BES Cyber System (BCS) which may contain BCSI):…” or similar language to to clearly establish the focus on BCSI.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

While having BCSI in the applicability column provides clarity, it unfortunately expands the scope of the requirements beyond what they are today. If the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment
We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems except for the initial 1.1. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to ‘Applicable Systems’. Recommendation: All parts of R1 needs to go back to “Applicable Systems”, The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems)“ R3 needs to stay, ‘Applicable Systems’.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA finds the proposed language is a significant change, and entities (and possibly auditors) do not have experience in applying this requirement to information. This may cause some confusion. CIP-011 is an information protection standard and it is sensible to put such a requirement here. Referring to the CIA model of Confidentiality, Integrity, and Availability, cyber security methodology often differentiates between protecting systems functionality/availability, vs. data. It is sometimes desirable to share data while still protecting the system from unauthorized use. If the SDT’s intent is to address distinct protections for data that may be processed, stored, or transmitted by the system separately from configuration information about the system itself (i.e., versions, settings, and runtime parameters), the definition of “Cyber Assets” (NERC Glossary pg. 10) should be examined to further clarify which and to what extent “data in those devices” is subject to which requirement.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	

We agree it clarifies the focus is on protecting the information, however we disagree that is the right focus for this type of standard. With the focus on BCSI comes the issue that the requirements are now impossible to measure on every piece of BCSI everywhere. It is only measurable at BCSI storage locations or repositories. *See answer to Question 2 for additional explanation.*

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	No
Document Name	

Comment

While providing better clarity it may expands the scope of requirements beyond what are in place today.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf.

Additionally, SDG&E would like to comment on CIP-011-3 requirement's proposed inclusion of all Medium-Impact BCS, regardless of ERC. The current CIP-004-6 R4.4 requirement specifies applicability for only High Impact BCS and Medium Impact BCS with ERC. The new CIP 011-3 brings all BCSI in scope regardless of ERC in Medium-Impact Sites. This change is significant and overburdensome to sites that don't currently fall into this category of BCSI.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No

Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We disagree with any and all Applicability that does not include the qualifying language "with ERC" for Medium Impact BES Cyber Systems except for the initial 1.1. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to 'Applicable Systems'. *Recommendation: All parts of R1 needs to go back to "Applicable Systems", The "Applicability" for R2, is acceptable. Add clarity to the R2 Applicability with "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems)" R3 needs to stay, 'Applicable Systems'.*	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
While we understand the reasoning behind the change, we feel that this change adds confusion and inconsistencies between CIP-011 and the rest of the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Please provide more clarity on the phrase "System information pertaining to". This needs to be well defined and understood. There may be many systems that are associated with systems that may or may not house BCSI.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE supports the comments as submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports adding BSCI in the Applicability Column of CIP-011-3. However, there are concerns with expanding the applicability to PCAs and Medium Impact BES Cyber Security Systems. First, in evaluating the proposed revision against the approved SAR, we are unable to find language to support the proposed revision. Second, the SDT should provide support that this modification will alleviate a reliability gap. Specifically, we ask the SDT to provide information regarding the reliability gap the proposed modifications are intended to address. Alternatively, the SDT could study the issue and develop a white paper, to identify, justify and explain the gap that they believe exists and, if necessary, revise the SAR.	
Likes 0	
Dislikes 0	
Response	

Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
NYISO understands the intent of the change. However, we are concerned that this would create an inconsistency in format with the other current CIP standards. NYISO would propose keeping the original “Applicable Systems” title and adding language such as “System Information pertaining to:” at the head (or similar) of each applicable row in requirements R1 and R2.	
Likes 0	

Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI’s comments	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems, except for R1 Part 1.1, if restricted to identifying BCSI, and the identification of BCSI storage locations, or Repositories, is broken out into a separate part (with Applicability to include “with ERC”) per Q1 response. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to “Applicable Systems.” Recommendation: All parts of R1 need to go back to “Applicable Systems.” The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems).” R3 needs to stay “Applicable Systems.”	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We disagree with any and all Applicability that does not include the qualifying language “with ERC” for Medium Impact BES Cyber Systems, except for R1 Part 1.1, if restricted to identifying BCSI, and the identification of BCSI storage locations, or Repositories, is broken out into a separate part (with Applicability to include “with ERC”) per Q1 response. The proposed language does not provide more clarity and needs to be more specific, not referencing another part. We recommend going back to “Applicable Systems.”

Recommendation: All parts of R1 need to go back to “Applicable Systems.” The “Applicability” for R2, is acceptable. Add clarity to the R2 Applicability with “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to: (Applicable Systems).” R3 needs to stay “Applicable Systems.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

IPC does not agree with the change from “Applicable Systems” (High Impact BES Cyber Systems and their associated: EACMS and PACS, etc.) to “Applicability” (BES Cyber System Information as identified in Requirement R1 Part 1.1) nor any reference other than an “Applicable System” reference in the “Applicable Systems” column. IPC believes the “Applicable Systems” language and approach should remain consistent across all CIP Standards. IPC does not agree that this change provides better clarity on the focus of the requirements; rather, this changes introduces and creates ambiguity and inconsistencies across the CIP Standards.

Likes 0	
Dislikes 0	

Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Because the definition of BCSI is left for the most part up to the entity this could lead to confusion during an audit if the auditor has a different interpretation for BCSI.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: Specification of information as an undefined category (i.e. “system information”) does not support understanding the intention of the information protections being addressed. The shift to an information protection standard is welcome, but would require some support of identifying types of information and developing some sort of inventory that can allow for concrete demonstration of protections and measures to comply. An entity could use a narrow interpretation of “system information” to overtly restrict what is considered BCSI and minimize the compliance burden at the expense of providing information protections. Since the rest of CIP-011-3 R1 depends on R1.1 identification, this could remove most information relevant to protection of cyber assets from consideration for compliance.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	

No comments

Likes 0	
Dislikes 0	

Response

William Hutchison - Southern Illinois Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Comments: Yes, it would be good to have BCSI in the “Applicability” column. We feel BCSI repositories need to have a significant explanation in the “Guidelines and Technical Basis” section as stated in question 1.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees that adding BCSI in the “Applicability” column provides further clarity on the focus of the requirements. However, Duke Energy suggests using the High and Medium designations carried with the applicability for consistency throughout the rest of the standards. Also, including the term “system information” in the applicability column and BES CSI in the requirement column may introduce scope ambiguity, particularly, for example, PCA is included in the applicability, but is not included in the NERC Glossary term BES CSI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment

Agree with proposing to have BCSI in the “Applicability” column and it is much clearer than the

current version since the CIP-011 requirements actually apply to BCSI rather than BCS and their

assocated cyber assets.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

That is fine as long as the Applicability section for R1.1 is worded correctly. We do not support introducing "System information pertaining to" in the applicability section for R1.1. This creates some ambiguity. We believe that the applicability be limited to BCSI.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment

AEP is in agreement that there is an overall increase in clarity on the focus of the standard. However, we were unable to find a justification for the change within the Technical Rationale and have concerns regarding the need for these modifications.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes

Document Name	
Comment	
Yes, it would be good to have BCSI in the “Applicability” column. We feel BCSI repositories need to have a significant explanation in the “Guidelines and Technical Basis” section as stated in question 1.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
The intention is good, and provides greater focus, however, the current proposed requirements still have some ambiguity due to the applicability of Requirement R1 including the BES Cyber System and associated Cyber Asset construct as the target.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	

Comment	
N&ST suggests deleting the word, “System,” thereby changing, “System information pertaining,…” to “Information pertaining,…”	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the proposed change as long as the change is coordinated with Project 2016-02 so there is consistency across all CIP standards.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	

Yes. We do agree. But does that mean NERC/FERC will consider the applicability section? They don't consider the applicability section related to CIP-002 IRC 2.11 they and FERC claim that non-BES generation is to be considered when performing a nRP evaluation of a GOP Control Center. The Applicability Section says "All BES Facilities". Why is the other CIP drafting team having to redefine BES in the new IRC 2.12. Is NERC and FERC going to pull a fast one again and say entities need to include non-BES Cyber Information in their BCSI Protection Plans?????

- And BES Means BES not non-BES
- and Facilities mean BES equipment not non-BES equipment
- and GOP's don't have GOP functional obligations for non-BES generation.
- Non-GOPs are doing just fine not providing GOP functional obligation services to non-BES generation and so are GOPs; i.e. neither GOP's and non-GOPs have GOP function obligations to any non-BES generator!. We reserve our GOP services for Generation Facilities (I.e. BES by NERC Glossary definition for Facilities and GOP's provide services to a operate Facilities) not non-BES assets, see definition of GOP in NERC Glossary of Terms.
- According to NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standrd are the (1) Applicability, (2) Requirements, and (3) effective dates.
- What good is the Applicability Section if NERC/FERC are going to ignore it?
-

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	Yes
Document Name	

Comment

Yes. However, consistency is important when defining and using terms. Please pick a single descriptor and use it consistently throughout. e.g. BCSI vs BES Cyber System Information.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	Yes

Document Name	
Comment	
We agree with the approach. Retitling the column to “Applicability” will be beneficial for all Standards and Requirements to allow for more flexibility. This aligns well with the work of the Project 2016-02 Standard Drafting Team that is also introducing new applicability. There may be future instances where the applicability cannot be limited down to a system.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

We do agree. But does that mean NERC/FERC will consider the applicability section? They don't consider the applicability section related to CIP-002 IRC 2.11 they and FERC claim that non-BES generation is to be considered when performing a nRP evaluation of a GOP Control Center. The Applicability Section says "All BES Facilities".

- And BES Means BES not non-BES
- and Facilities mean BES equipment not non-BES equipment
- and GOP's don't have GOP functional obligations for non-BES generation.
- Non-GOPs are doing just fine not providing GOP functional obligation services to non-BES generation and so are GOP. We reserve our GOP services for Facilities nor non-BES assets.
- According to NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standrd are the (1) Applicability, (2) Requirements, and (3) effective dates.

What good is the Applicability Section if NERC/FERC are going to ignore it?

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT agrees with this approach. Retitling the column to “Applicability” will be beneficial for all Standards and Requirements, and allow for more flexibility. This revision aligns well with the work of the Project 2016-02 Standard Drafting Team that is also introducing new applicability. There may be future instances where the applicability cannot be limited down to a system.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment
PG&E agrees with the Applicability change to “System Information pertaining to” is appropriate and provides clarity on what is to be protected. PG&E has concerns about the addition of PCA to the “System Information” to be protected. The concern is the additional effort to identify and protect this information and the potential benefit of those additional protections. PG&AE is requesting the SDT articulate the reason for the proposed addition of PCA since there is no information in the Technical Rationale document to warrant its addition.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	

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 NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
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	
Bradley Collard - SunPower - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	
Document Name	
Comment	
Neither agree nor disagree	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	

Comment

How are entities to list NERC, Regional Entities, FERC, etc.? The Standard should allow certain exemptions. They should also allow for exemptions post NERC Exceptional Circumstance incidents where the information may be shared to expedite recovery.

Agree with Tarantino's comment about this needs to be included in CIP-013.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	

Comment

Comments:

Requirement R1

The language in R1.4 goes beyond providing an opportunity for a Responsible Entity to address appropriate security controls because it requires remediation and mitigation actions, including planned date of completion and status on action items. The requirement should also note that the risk assessment is only necessary when a vendor or other third-party is housing the information. In other words, the assessment should not be required if the information is stored by the Responsible Entity on its premises.

Additionally, the CIP-011 requirements seem to toggle from objective-based requirements to prescriptive-based implementation activities in an unstructured manner. For example: R1.3 (Process to authorize access to BCSI) is objective-based, but R1.5 (Revoke the individual's current access to BCSI by the end of the next calendar day following the effective date of the termination) is prescriptive-based. R1.5 also implies that the process to authorize access to BCSI must be on an individual (person by person) basis, which brings us right back the issue with CIP-004 and having BCSI in the Cloud when an Entity may not have a list of individuals with access to the information. An Entity should be able to authorize a company, vendor, individual, etc. to access information and it should have the flexibility to define how it implements the authorization process.

Requirement R2

The Standards should remain technology neutral. By prescribing key control management programs, there is an assumption that key management is the only way to address preventing the ability to obtain and use BCSI through unauthorized access. Again, the requirements toggle between objective-based and prescriptive/technology-based.

Recommendation: the SDT should consider either including information protection measures for vendors in CIP-013, or approaching CIP-011 similarly to CIP-013. Specifically, the SDT should consider creating a requirement to develop and implement a BCSI security risk assessment plan and describe the criteria that should be included in the plan (for example, a process to authorize access, a process to prevent ability to obtain and use BCSI from unauthorized access, a process to revoke access within the next calendar day, etc.). This approach allows an Entity:

- to focus on identifying information security risks and objectives specific to its needs and appropriately addressing them;
- flexibility and scalability regarding how to implement technical controls, as well as remediation & mitigation activities; and
- the ability to leverage emerging technologies that might better address information security risks without requiring updates to CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The way the requirement is currently written there is confusion between how R2 will be applied to on premise storage solutions. The “Where Applicable” reference does not fully explain the types of storage locations referred to in the requirement.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013.

We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive.

Similar to the explanation of the term “vendor(s)” in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E agrees that R1 P1.4 and R2 are a good start in addressing the security risks of BCSI but is concerned with the apparent overlap that P1.4 has with CIP-013 Supply Chain Risk Management R1 P1.1 risk assessment. Could CIP-011 SDT just reference the CIP-013 requirements for vendor risk assessment and allow the entity to determine the appropriate method(s) for determining the risk, documentation of the risks and frequency of re-assessment based on their CIP-013 plan(s)?

PG&E also has a concern regarding the language of Requirement R2. PG&E believes that it is not clear if key management is for physical, electronic, or both types of keys. This lack of clarity could lead to entity confusion on what is covered. The Technical Rationale document for Requirement R2 does indicate it covers both, but we are aware the Technical Rationale document is not always read and does not carry the same compliance mandate as Requirement language.

PG&E recommends the Requirement language clearly indicates key management should cover such items as physical and electronic keys, with the “such as” proceeding the “such as” to possibility future proof the Requirement to technology changes we are not aware of yet.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Regarding Part 1.4, this requirement appears to be better addressed in CIP-013. ERCOT refers the drafting team to ERCOT's comments in response to Question No. 3 recommends excluding applicability of all requirements for cloud service providers, but including the minimum requirements in the cloud vendor risk assessments of Part 1.4.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013. We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive. Similar to the explanation of the term "vendor(s)" in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
This is way too prescriptive. Vendor requirements should reside only in CIP-014.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	

Comment
Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	

Comment
While the proposed changes to promote a better understanding of the security risks, they are not in alignment with the current CIP-013-1 Standard for Supply Chain Risk Management. Third-parties are part of the supply chain, and adding a Supply Chain Risk Management (SCRM) requirement within CIP-011-2 R1 Part 1.4 adds unnecessary ambiguity and double jeopardy with Cloud Providers SCRM requirements falling under both CIP-013-1 and CIP-011-3. Additionally, the R2 requirements add additional ambiguity in their applicability. R2 Part 2.1 has a “where applicable” clause which seems to alleviate the compliance burden for an entity that does not use PKI or like key management. Part 2.2 does not have this “where applicable” clause, but relies on duties identified in Part 2.1, which would still apply to an entity without PKI, but what are the compliance requirements in this case? Additionally, R2 imposes a significant burden on an entity who has key management infrastructure and local only BCSI storage. If there is key management infrastructure at the enterprise level, this does not mean that the entity is capable of implementing this infrastructure to encrypt local BCSI storage locations using the PKI, nor is there a requirement to do so. However there would be a requirement to implement documented processes supporting R2 for an infrastructure that has no relevance to the BCSI.

A possible solution to this issue would be to modify the applicability to “BCSI from R1 Part 1.1 that is encrypted using a key management infrastructure” or similar.

OR to change the R2 level language to something similar to this:

“Each Responsible Entity shall implement one or more documented key management programs that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection, for key management infrastructure used to protect BCSI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].”

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2

Answer	No
Document Name	

Comment

PGE agrees with EEI’s comments

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

Regarding Part 1.4, this requirement appears to be better addressed through CIP-013. Please see comments to question #3. Recommend to exclude applicability of all requirements for cloud service providers and include the minimum requirements in the cloud vendor risk assessments of R1.4.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No

Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments. Specifically, if key management is not a requirement (due to the "where applicable" language in 2.1), then it is not appropriate to have this language in the requirements section and would be better suited to guidance. The requirements should only state what is required.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the fundamental requirements and reasoning behind the proposed additions but believe it would be better placed within the context of CIP-013 vendor and supply chain risk management. CIP-011 should be limited to information handling and protection. Vendor vetting and management would appear to fit better within the overall context of CIP-013.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
This is way too prescriptive. Vendor requirements should only reside in CIP-014.	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	

Answer	No
Document Name	

Comment

If the intent of the proposed changes to CIP-011-3, requirement R1, Part 1.4 is to better understand and mitigate assessed risks to BCSI being stored within a vendor-managed environment, NYISO believes the proposed changes are potentially overly broad and administratively burdensome in comparison to risks currently assessed under CIP-013-1.

As stated in our response to question #3, NYISO would recommend eliminating Part 1.4 of requirement R1 from CIP-011-3. The issue of risk assessments for vendors could be addressed as part of Project 2019-03: Cyber Security Supply Chain Risks (i.e. CIP-013-2), this would have the benefit of accounting for all vendor requirements (BCS and BCSI) within the same standard.

Regarding examples contained within CIP-011-3, requirement R2, Parts 2.1 and 2.2, a key management process is an example of one method that could be applied to prevent unauthorized access. NYISO feels that this example would be better included under requirement R1. NYISO proposes requirement R2 be removed from the current draft.

Another suggested consideration would be include protections of BCSI stored in environments owned or managed by third parties into a separate requirement. For example, combine the requirements into “R4”, which could reference R2 (Key management) as a stated requirement (not optional) for BCSI stored in environments owned or managed by third parties.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

There are other more appropriate methods to “promote better understanding” of issues and topics than through the standards drafting process. Perhaps such issues and topics could be included as part of a Technical Rationale, supporting white paper, or using other available mechanisms.

With regard to CIP-011-3, Requirement R1, Part 1.4, the requirements appear to duplicate CIP-013 Requirements. As such, we would encourage the SDT to address a perceived security gap of BCSI stored at third party facilities within the CIP-013-1 Standard.

Regarding CIP-011-3, Requirement R2, Parts 2.1 and 2.2; EEI offers the following comments:

The SDT is prescribing requirements that do not appear to conform to NERC guidance regarding development of results-based Reliability Standards. While encryption and key management would be an acceptable method for ensuring the security of BSCI at third party facilities, specifying this solution within requirements may be overly prescriptive and potentially limit entities from using other methods to secure BCSI, if future technology advancements offer such solutions. For this reason, the language should be broader with less prescription. If the SDT believes that the requirements as described in R2 must be pursued, EEI suggests the following:

Part 2.1: “Where applicable” should be more clearly defined in order to avoid any confusion as to when key management processes are required, otherwise the list of processes appears to be sufficiently comprehensive to ensure the security of BSCI.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

If the SDT’s intent is to address security risks associated with vendors, then that should be specifically expressed in the requirements. The current language is vague and needs further clarification. Part 1.4 states “in cases where vendors store” but Part 2.1 and Part 2.2 do not. In Part 2.1, the statement “where applicable” needs to be expanded to clearly provide when a key management program must be implemented. As written, the proposed requirements are too broad and could add an undue burden if auditors take the broadest possible meaning. Part 2.2 is not clear due to the vagueness of Part 2.1. The following changes are suggested;

“Part 2.1 When BCSI is stored in environments owned or managed by vendors, develop a key management process(es) …”

“Part 2.2 When BCSI is stored in environments owned or managed by vendors, implement controls to separate …”

Also in reference to Part 2.2, the phrase “BCSI custodial entities duties” is not clear and open to broad interpretation.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No – if the intent of the proposed changes to CIP-011-3, requirement R1, Part 1.4 is to mitigate risks particular to BCSI stored in a vendor managed environment, MISO believes the proposed changes are overly broad and administratively burdensome in comparison to those risks currently assessed under CIP-013-1 and the small amount of incremental benefit gained in relation to the level of effort required to produce it.

MISO recommends eliminating Part 1.4 of requirement R1 from CIP-011-3 and recommends the issue of risk assessments for vendors be addressed as part of Project 2019-03: Cyber Security Supply Chain Risks (i.e. CIP-013-2), thereby covering all vendor requirements (BCS and BCSI) in the same standard.

Regarding proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2, a key management process is an example of one method to prevent unauthorized access and would be better included as an example under requirement R1. MISO proposes requirement R2 be eliminated altogether.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
To avoid confusion and the splitting of requirements, vendor risk management, including risk assessments of vendors, should be included in CIP-013. Additionally, the concept of assessing the risk of cloud-providers is good, but the execution within the requirements needs more work. For instance, the requirement is unclear on what constitutes a vendor “storing” an entity’s BCSI, and an auditor could make the assumption that this requirement applies to all vendors and systems and not just to cloud providers. Another example is the timeframe described in Part 1.4.2. This timeline implies that BCSI is more important than the actual BES Cyber Assets themselves (as CIP-013 has no timeframe for reassessments).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment

1. We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. See #2 for more feedback. NYPA is voting ‘NO’ based on these apprehensions.
2. We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan. The potential costs of these controls may not produce an effective result. Plus the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review instead of a trigger.
3. We request this SDT consider if these vendor controls (mitigations) belong in CIP-013.
4. We request clarification of physical security - will Part 2.2 be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

We believe R1 Part 1.4, and R2 Parts 2.1 and 2.2, exceed the scope of the SAR. We agree with EEI comments that vendor risk assessments with respect to hosting BCSI should be addressed with a modification to CIP-013.

We concur with EEI comments that the draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive.

Similar to the explanation of the term "vendor(s)" in the CIP-013 Supplemental Material, it must be made clear with respect to vendors in R1 Part 1.4, and custodial entity in R2 Part 2.2, that Regional and Registered Entities, as well as NERC and FERC, are exempted as such.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

1. We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan.
2. We request this SDT consider if these vendor controls (mitigations) belong in CIP-013.
3. We request clarification of physical security. Part 2.2 may be difficult to implement where the custodian and the person with the key are the same.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
The BCSI should be protected regarless where it is. When and how to perform risk assessments of the vendors that store the Responsible Entity's BCSI should not become an extra burnden on Responsible Entity.	
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	
R1.4: Southern believes the wording "Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information" is less clear. This has no wording to scope it to off-premise situations. Vendors produce all types of data storage solutions and this could be interpreted to mean that all BCSI is stored by a vendor. The requirement should specify the relationship the vendor has to the "storing" of the data as we believe this is about when vendors own/operate/maintain the storage in an off-premise cloud service environment. R2: Requires that an entity "**shall implement** one or more documented key management program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection" regardless of whether or not an entity encrypts its BCSI or not. For entities that keep all BCSI on-premises and choose to not use 3rd party cloud solutions or encryption as a technical control, this main R requirement serves no purpose, and results in a documentation exercise to 'prove the negative.' Consider moving the term "where applicable" to the main R requirement to explicitly exempt those entities that do use encryption as a technical control to protect BCSI in storage, transit, or use.	

Overall, Southern believes that the R2 requirements for VRA's should be part of CIP-013 which is a more holistic approach to vendor risk. We do not agree with the need to piecemeal different flavors of VRAs throughout the CIP standards for individual technical areas. CIP-013-1 R2 currently has language containing a cyber security risk management plan for supply chain. We suggest this be removed from the proposed CIP-011 and instead be coordinated with the Supply Chain SDT to add language or a requirement to align with conducting vendor risk assessments.

Part 1.4 seems to be somewhat a duplication of 1.6 where a verification of access to BCSI is required on the same time interval.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. Supply chain related related requirements should remain as part of the CIP-013 planning process.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
“System Information Pertaining to” BCS is far too vague. The NERC Glossary definition of BCSI shows examples rather than a principle by which to designate BCSI. Guidance on this point fails to approach data “classification” or “categorization” according to sound and well-developed principles in widespread use for which expertise and guidance exists from the Intelligence community. One vital concept is aggregation of data leading to increased risk. The glossary definition gives an example or hints at it through the phrase “collections of network addresses:” but doesn’t explain how an Entity would create a guideline for policy that assesses risk based on aggregation, doesn’t discuss “Essential Elements of (Friendly) Information” concepts and doesn’t discuss derivative classification and marking.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We believe R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR. Vendor risk assessments are addressed in CIP-013. The result of identifying, assessing, and mitigating vendor risks is still going to be controls we implement to prevent unauthorized access, which is already required in various other current CIP Standards. The concern is that the SDT is developing a requirement that is duplicative of requirements contained within CIP-013, and any modifications should be addressed in that Standard, not in CIP-011-3.	

If R1 Part 1.4 needs to be pursued in CIP-011, per the definition of a Vendor in CIP-013, Regional and Registered Entities, need to be exempted from being regarded as vendors, suppliers, or custodial entities.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that, following the Effective Date of 7/1/20 for CIP-013, vendors offering BCSI storage services will be subject to that Standard, which in our view renders proposed CIP-011-3 Requirement R1, Part 1.4 redundant. Moreover, the proposed requirement is more stringent than any requirement in CIP-013! The SDT is, in essence, proposing to require Responsible Entities to perform ANNUAL vulnerability assessments of their cloud storage vendors (if any). N&ST admits to being hard-pressed to imagine how a Responsible Entity could perform a credible “risk assessment” of, for instance, Microsoft Azure beyond asking them in writing if they still have the same FedRAMP authorization level as they had the previous year. The “Technical Rationale for Reliability Standard CIP-011-3” includes a statement, “If the focus is protection of BCSI, the device or storage location becomes less relevant,” that seems inconsistent with the proposed “risk assessment” requirement. N&ST recommends that it be dropped.

With regards to proposed Requirement R2, Parts 2.1 and 2.2, N&ST considers them vastly over-prescriptive. The goal here is to ensure that no individuals who manage BCSI storage, whether in the Responsible Entity’s own data center or “in the cloud,” can access BCSI unless they have been properly authorized in accordance with the requirements of CIP-004. Encryption and key management are certainly viable options, but they should remain options. N&ST suggests moving them to the “Measures” associated with an appropriately re-worded requirement.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	No
Document Name	

Comment

While Tri-State G&T agrees with the concept of performing a risk evaluation (proposed by Part 1.4) associated with a cloud solution, we do not agree it needs to be a compliance requirement. We think that the other requirements (access management, methods to protect/secure BCSI, etc.) already force the Registered Entity to evaluate and identify risks, possible solutions, etc. Making the risk evaluation a mandatory requirement does not add value, and instead adds unnecessary adminstrative compliance burden.

The R2 requirements as drafted are entirely too prescriptive and should instead be converted to objective-based requirements. Furthermore, as to R2.2, entity’s should be permitted to have the same vendor manage the keys and hold the encrypted data, as long as controls are in place to prevent

unauthorized access and detect when an unauthorized action has been taken. Additionally, the use of the phrase “Where applicable” should be clarified. We recommend instead using the phrase “Where encryption is utilized as a method to restrict access to BCSI”.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

The proposed language for CIP-011-3, Requirements R1, Part 1.4 are not only duplicative of CIP-013, they also prescribe mandatory timeframes for the performance of periodic risk assessments for what is otherwise an objective based standard in CIP-013. This periodicity should be left up to each Registered Entity to define within their Supply Chain Risk Management plan. To remove double jeopardy, prevent confusion, and maintain consistency for supplier risk management requirements, CIP-011-3, Requirements R1, Part 1.4 should be removed and cloud-based suppliers for BCSI should be covered in CIP-013.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	

Comment

AZPS agrees that the proposed language in Part 1.4 addresses security risks associated with instances where a vendor stores a Responsible Entity’s BCSI. However, Parts 1.4.1 through 1.4.3 introduce duplicative requirements to perform risk assessments, as the requirement will be satisfactorily met with the implementation of CIP-013-1 Part 1.1. AZPS recommends retaining Part 1.4 and remove sub-parts 1.4.1 through 1.4.3.

With respect to CIP-011-3 R2, AZPS provides its response in Question No. 8.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Requirement R1 Part 1.4 is a step in the right direction for structuring a framework that considers third-party providers as a viable source. However, as written, the language falls short in the following wasy:

- This entire process should be included in the CIP-013 Supply Chain standard that already deals with bendor risk assessments, etc. This is duplicative to that effort and one that would likely be collapsed into CIP-013 during a subsequent efficiency review
- The intent to mitigate risk does not include the intended risk threshold or objective. If this is to be determined by the entity, the outcome should be clearly indicated. If this risk analysis were included in CIP-013, the entity already defines the process and risk objectives there, so this would also be a duplication.
- Part 1.4.3 - is it necessary to state that the entity needs to "document the results of the risk assessment"? This serves as a Measure to Part 1.4.2 than a standalone requirement, which in and of itself, is administrative. Furthermore, Part 1.4.3 should be reworded to state, "Implement an action plan to remediate or mitigate risk(s) identified in the risk assessment performed according to Parts 1.4.1 and 1.4.2, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items."
- Bullets 3 and 4 in the Measures - what is the difference between the "documentation of the vendor risk assessments" and "documentation of the results of the vendor risk assessments"? It seems these could be combined into a singular measure.

With respect to R2 Parts 2.1 and 2.2:

- The objective is to restrict access but it is not clear to what? The requirement should be clarified. Is the key management process intended for physical access to locations of BCSI storage locations? Electronic access to folders and/or information containing BCSI? Both? Something else? This appears to be an available Measure to meet Part 1.2 and not an independent requirement covering the same reliability objective of preventing unauthorized access.
- There are several terms included in the Parts 2.1.1 - 2.1.9 list that are not commonly understood without further explanation (e.g. key suppression, periods). These need to be presented or explained more clearly to inform the Registered Entity what the intent is.
- In Part 2.2, the use of "custodial entity" is not well understood. Furthermore, the intended security objective of this requirement is not clear as a result.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

These additional requirements should be added to the language of CIP-013 and addressed in the entities supply chain risk management plan. Do not mix the standards requirements.

Likes 0	
Dislikes 0	

Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Yes, agree that a stand alone requirement where a vendor stores an entitiy's BCSI is needed. 1.4.1 requires an initial risk assessment of vendors but the SDT needs to define what is acceptable evidence for a risk assessment. Is requirement 2 only applicable to BCSI stored in the cloud? For R2.1 the SDT should define key management and provide guidance in a GTB. For R2.2 if an entity uses secure thumdrives, how can they separate the duties? Who in this requirement is the custodial entity?	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Doing a risk assessment of an 3rd party / offsite storage provider is practically useless. The best a RE will get from most providers is a SOC1 or SOC-2 report. The way this is written today only creates compliance risk and burden on the RE. The majority of offsite/Cloud provider storage solutions (a majority if not all the providers RE's would use) are not the issue when it comes to security risks. These types of businesses would not be in business if they did not have strong security systems in place and would not be used by Federal, State, Local governments and Fortune ranked companies. Instead of putting the burden on the RE, NERC/FERC needs create an approval process and keep an approved published list of 3rd party storage vendors list for RE's to be able to use. This is exactly what is done for government and government contractors. This would be more efficient, more in-depth, and not create compliance burden on the RE's. This would not restrict competition or violate any laws as any 3rd party would be able to go through the process to get approved. In almost all documented cloud data breach cases we are aware of, it has been the end user which has caused data leaks not the provider themselves ref: https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203 . We followed this article up by asking various cybersecurity experts from EY, Mandiant, and Cisco. The only compromise which came up from them was 3rd party identity providers. The compromise was of their own outward facing application and not the security of or compromise of customer storage solutions. The greater risk in cloud/3rd party storage solutions lies more in a customer not having the knowledge of the risks and security tools necessary to protect data in the cloud than the cloud provider itself. This is also significantly dependent on the type of environment being used such as a completely private cloud vs hybrid public/private cloud and its subsequent configuration	
Likes 0	

Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the proposed revisions will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls; however, it does not support the manner in which the proposed requirements do so. Specifically, GSOC is concerned about introducing a separate vendor risk assessment for vendors under CIP-011 than is proposed in CIP-013. Such segregation of similar and potentially related requirements and processes into 2 different standards introduces (rather than reduces) overall risk as discussed below in GSOC's response to question #10. If a risk assessment for a vendor is necessary, then, the team should work with the Supply Chain SDT to modify CIP-013. This is especially important where cloud services are provided under a master or general services agreement that is in scope for CIP-013 as an additional requirement under CIP-011 creates redundancy and the potential for error. Further GSOC notes that mitigations are not required to be implemented in CIP-013, but are required to be implemented here for what is likely a less risky procurement. It is unclear as to why this would be necessary and, as this is not addressed within the Technical guidance, it should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to require a separate risk assessment and mandatory risk mitigation within CIP-011 for access to information when mandatory mitigation is not required within CIP-013.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment
R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR and significantly increase the compliance obligations. CIP-011 should remain non-prescriptive and allow entities to implement the controls appropriate to their situations. Vendor risk assessments are addressed in CIP-013 and should not be required here. In any case, the end result of identifying, assessing, and mitigating vendor risks is still going to be the controls we implement to try and prevent unauthorized access, which is already required by CIP-011. It is also unclear as to when/if these requirements are applicable.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
NRECA agrees that the proposed revisions will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls; however, it does not support the way the proposed requirements do so. Specifically, NRECA is concerned about introducing a separate vendor risk assessment for vendors under CIP-011 than is proposed in CIP-013. Such segregation of similar and potentially related requirements and processes into 2 different standards introduces (rather than reduces) overall risk as discussed below in NRECA's response to question #10. If a risk assessment for a vendor is necessary, then, the team should work with the Supply Chain SDT to modify CIP-013. This is especially important where cloud services are provided under a master or general services agreement that is in scope for CIP-013 as an additional requirement under CIP-011 creates redundancy and the potential for error. Further, NRECA notes that mitigations are not required to be implemented in CIP-013, but are required to be implemented here for what is likely a less risky procurement. It is unclear as to why this would be necessary and, as this is not addressed within the Technical Rationale, it should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to require a separate risk assessment and mandatory risk mitigation within CIP-011 for access to information when mandatory mitigation is not required within CIP-013.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
Regarding CIP-011, Requirement 1, Part 1.4, AEP feels that this requirement does not belong in CIP-011. We believe vendor management/supply chain requirements belong in CIP-013 rather than CIP-011. If the current language in CIP-013 does not address BCSI protection when stored at a third party location, AEP recommends modifying the CIP-013 standard to address these needs. In regards to CIP-011, Requirement 2, Parts 2.1 and 2.2, AEP is of the opinion that key management and encryption may not be enough to properly ensure the protection of BCSI when being stored in a third party facility. We also feel these requirements could use some clarification regarding when it's necessary to use key management methods. AEP is unsure of how "where applicable" is defined within Part 2.1, which could lead to insufficient protection of BCSI based on how that phrase is interpreted.	
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 focus needs to be on protecting access to the information. This should be performed in a vendor/platform neutral manner - whether the systems are administered by in-house personnel or hosted on a shared cloud-based hosting provider, the outcome, regardless, should be that access to the information is limited to authorized individuals only. The risk assessment is an additional undue burden on the entity that the existing process should account for regardless of the outside party the information is being shared with. As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions, and to apply regardless of the outside party with whom the information is shared.	
Likes 0	
Dislikes 0	
Response	

Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

While Tri-State agrees with the concept of performing a risk evaluation (proposed by Part 1.4) associated with a cloud solution, we do not agree it needs to be a compliance requirement. We think that the other requirements (access management, methods to protect/secure BCSI, etc.) already force the Registered Entity to evaluate and identify risks, possible solutions, etc. Making the risk evaluation a mandatory requirement does not add value, and instead adds unnecessary adminstrative compliance burden.

The R2 requirements as drafted are entirely too prescriptive and should instead be converted to objective-based requirements. Furthermore, as to R2.2, entity's should be permitted to have the same vendor manage the keys and hold the encrypted data, as long as controls are in place to prevent unauthorized access and detect when an unauthorized action has been taken. Additionally, the use of the phrase "Where applicable" should be clarified. We recommend instead using the phrase "Where encryption is utilized as a method to restrict access to BCSI".

Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	

Seattle is concerned about the overlap and potential for conflict between proposed CIP-011 vendor controls and CIP-013. Seattle prefers an objective-based, risk-focused approach that would leverage CIP-013 controls without restating them. Depending on how an entity used, transports, and stores its BCSI, additional controls might be warranted for third parties involved in BCSI processes, but these might be better left up to each entity to determine and defend, based on existing security concepts. For example, an entity may determine that a third-party with a valid FedRAMP certification is sufficiently risk-free to engage to store BCSI, or it might identify specific individual controls. Leaving it up to each entity, with some reasonable guidance, serves to break the Gordian Knot of third-party certifications that to date has stifled most NERC approaches to third party storage providers.

Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment
The requirement language is not clear as SDT expected. If it is intended that R1 Part 1.4 and R2 only apply when vendors are involved, the Requirement language should clearly state this. In addition, for R1 Part 1.4 and R2 Part 2.2, Regional and Registered Entities, as well as NERC and MRO, need to be exempted from any possibility of being regarded as vendors or custodial entities. R2 requires entities to have a key management program, but the wording regarding encryption and vendors are missing. Suggest adding the following language to R2: "… shall implement one or more documented key management program where vendors are custodians and BCSI are encrypted…" In R2 Part 2.1, we believe "key suppression" is a typo and it should be "key supersession". Also if it is intended to address the electronic key rather than physical key, it should clealy state electronic key or encryption key in the requirement language. In R2 Part 2.2, what does the term "custodial entity" mean? If this is a term taken from other guidance or standard documents (NIST, Cloud Security Alliance etc.), those should be referenced. Across various NIST and CSA documents, the terms "data custodian" and "key custodian" are both in use. In R2 Part 2.2, when separation of duties is being called for, it's not clear which particular duties must be kept separate. Also it is not clear whether the separation of duties means between the vendors and Registered Entities. In R2 Part 2.2, it is not clear if it is acceptable for a vendor to have both custody of data and ability to use it (e.g. have an encryption key.) if the vendor separate their staff's duties.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	

Comment
Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The language appears that the key management would be outside of the Responsible Entity. The Responsible Entity may manage their own keys in certain architectures. Clarification that separations are needed where an vendor (3rd party) is used for key management.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive. Key management should not be specified as the means, as there are others. R2 Part 2.1 should be deleted in its entirety. Also, for R1 Part 1.4 and R2 Part 2.2, Regional and Registered Entities, as well as NERC and FERC, need to be exempted from any possibility of being regarded as vendors or custodial entities.	

R1 Part 1.4 and R2 Parts 2.1 and 2.2 exceed the scope of the SAR. We do not believe this is an appropriate place to promote better understanding of security risks involved, nor do we think we should be held to these extremely prescriptive requirements. Identifying, assessing, and mitigating vendor risks will already be addressed as part of preventing unauthorized access.

How a Responsible Entity chooses to implement their access control program should not be prescribed within standard language. We suggest removing all language from CIP-011-3 R1.2, R1.4, R2.1 and R2.2. We believe that the inclusion of storing BCSI with cloud based service providers can be addressed by defining “BCSI Access” in the NERC Glossary of Terms. The definition language could be taken from the April 26, 2019 ERO Enterprise CMEP Practice Guide on BES Cyber System Information: “An instance or event during which a user obtains and uses BCSI. For access to occur, in this context, a user, authorized or unauthorized, must concurrently both obtain BCSI and possess the ability to use BCSI. An unauthorized individual who obtains encrypted BCSI but has no ability to use it within a meaningful timeframe should not be considered to have access.”

Currently CIP-004-6 adequately addresses access controls to BCSI when stored by the responsible entity. The issue with the current access requirements is when applied to offsite vendors due to the fact that the Responsible Entity cannot control a vendor’s access to the BCSI.

With this definition in place the SDT can then simply change CIP-004-6 R4 to read:

R4: Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances”:

4.1.1. Electronic Access

4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.1.3. BCSI Access

The SDT could also change language in CIP-004-6 R5.3 to read:

For termination actions, revoke the individual’s access to BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

Part CIP-004-7 R4.1.3 would limit “BCSI Access” appropriately to vendors that are custodians to encrypted or otherwise masked data but do not have the ability to use it. Any vendor with both custody of data and ability to use it (e.g. have an encryption key) would need to be provisioned access by the Responsible Entity through their established access control process and procedures.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

We recommend that CIP-013 is expanded to include vendors that store BES CSI on behalf of entities. The vendor requirements in CIP-011 exceed CIP-013 requirements may result in additional processes that can be covered by the CIP-013 standard.

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	

1. CIP-011 R1, Part 1.4 states "*Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information*…." Since MEAG does not store its BCSI in the cloud with another vendor, would this requirement be **N/A**, or does MEAG still need to develop a risk assessment document (program/process) in the event we decide to use a cloud vendor for our BCSI in the future?

2. CIP-011 R2 deals with a key management program. Is this for physical and/or cyber? This requirement seems to assume that all entities would have a key server for authentication, revocation, etc. Is this only for those entities that are using a 3rd party vendor to store BCSI? However, what about those entities that don't issue 'keys'. For example, MEAG encrypts its files on the MEAG shared drive, but it is protected only by a secure password that is given to only a 3 people; the IS Administrators can't even see the contents of the files. Does MEAG need to call the software vendor to ask how files are encrypted by the software and how the keys get processed on the PC? The encryption on the files works in the background; MEAG has no control on that process. So, can this requirement be N/A for MEAG Power? Will N/A be allowed by the Auditors?

Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy generally agrees that these requirements will promote a better understanding of security risks. Duke Energy would like better understanding of the opportunities to address appropriate security controls. Also, Duke Energy would like more clarity on what consitutues an acceptable risk assessment and/or what other options would suffice instead of a risk assessment.

Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	

Answer	No
Document Name	
Comment	
Comments: Doing a risk assessment of an 3rd party / offsite storage provider is practically useless. The best a RE will get from most providers is a SOC1 or SOC-2 report. The way this is written today only creates compliance risk and burden on the RE. The majority of offsite/Cloud provider storage solutions (a majority if not all the providers RE's would use) are not the issue when it comes to security risks. These types of businesses would not be in business if they did not have strong security systems in place and would not be used by Federal, State, Local governments and Fortune ranked companies. Instead of putting the burden on the RE, NERC/FERC needs create an approval process and keep an approved published list of 3rd party storage vendors list for RE's to be able to use. This is exactly what is done for government and government contractors. This would be more efficient, more in-depth, and not create compliance burden on the RE's. This would not restrict competition or violate any laws as any 3rd party would be able to go through the process to get approved.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
This type of requirement often becomes a problem during enforcement, when the auditors evaluate the quality of the assessments. This is a reoccuring issue with the auditors, and can only be resolved through more specific wording in the requirements.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided 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 NextEra	
Answer	Yes
Document Name	

Comment
1) We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. See #2 for more feedback. 2) We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls. Entities have little control of vendors OR the vendors of the primary vendors. We recommend the path laid out by CIP-013 – a) have a plan and b) implement that plan. The potential costs of these controls may not produce an effective result. Plus the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review instead of a trigger. 3) We request this SDT consider if these vendor controls (mitigations) belong in CIP-013. 4) No consensus on Part 2.1 5) We request clarification of physical security - will Part 2.2 be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
Texas RE recommends the SDT define the term “vendor”, which is used in Part 1.4 as well as referenced in CIP-005-6 and CIP-013-1. This would ensure an understanding of what is considered a vendor.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	

Comment
We believe the proposed vendor risk assessment is best under CIP-011 rather than combining with CIP-013.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment
IESO agrees in principle with the comments submitted by NPCC We agree with that Part 1.4 will promote a better understanding the security risks involved. We have serious concerns with these controls: 1. We have strong apprehensions on “mitigate” in Part 1.4 and possibly push some to vote NO on this project. Entities have little control of vendors their subcontractors vendors. We prefer the SDT consider that these vendor controls (mitigations) belong in CIP-013. If the SDT leaves these controls in CIP-011, we recommend the same type of strategy used in CIP-013 – a) have a plan and b) implement that plan rather that “mitigate” 2. In regards to Part 2.2 , we request clarification with respect to physical security - Part 2.2 may be difficult to implement where the custodian and the person with the key are the same?

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	

Comment
Please clarify if R1.4 would apply only to vendors providing storage as a service for BCSI, or if it would apply to any vendor possessing any amount of BCSI.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment

We would encourage the SDT to include a time frame for when 3rd party security mitigations need to be completed. It is an improvement to see that a date must be included for closure of identified security risks, but this is still open ended and will not ensure timely closure of risks.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	

Answer	
Document Name	
Comment	
We support NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
While this will promote a better understanding of the requirements, it suffers in that internally stored information does not require the same types of controls as externally stored information. For example, a company may encrypt all data storage, whether or not BCSI. However, requiring a separate key custody process for internally stored information in small registered entities is an excessive and overly prescriptive requirements.	
Likes 0	
Dislikes 0	
Response	

7. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

There is not enough detail to address large service providers who will not cooperate with an entity for risk assessments for cloud computing. Companies such as MicroSoft have not be very cooperative in helping us assure that the information is protected. All companies should be able to be held to a common standard.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The revisions make the use of specific technologies less apparent and adds to complexity. If cloud is permitted, it should list this as an example.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

As indicated in our previous responses, especially to Q3 and Q6, we believe that the proposed Requirements, by overly focusing on and prescribing technologies, will instead significantly increase administrative activities and costs as well as introduce significant new compliance risks, and may discouraging Responsible Entities from pursuing such options.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

Agree with SDT's idea and disagree with the written language that is vague. Cloud storage and encryption technologies are not explicitly excluded under the current standards, where the registered entity could include NDA or contract provisions that require vendors to provide BCSI access and handling evidence in order to meet CIP-011 and CIP-004 requirements. Even though the new requirements R1.4 and R2 try to provide other cloud services solutions, we haven't see the cloud storage and encryption language in the revised requirements.

SDT should focus on revising or developing new requirements that meet the objective of protecting access to BCSI without constraining or prescribing types of storage solutions such as physical and electronic access controls. Any new Requirements need to address cloud services should clearly state that in the requirement language.

Currently CIP-004-6 adequately addresses access controls to BCSI when stored by the responsible entity. The issue with the current access requirements is when applied to offsite vendors due to the fact that the Responsible Entity cannot control a vendor's access to the BCSI even though NDA could be used for the compliance.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle supports the comments of SMUD to this question.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

The changes do show support and leverage towards new and future technologies but they are too specific and do not provide flexibility for the various solutions and security controls that could vary.

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 focus needs to be on protecting access to the information. This should be performed in a vendor/platform neutral manner - whether the systems are administered by in-house personnel or hosted on a shared cloud-based hosting provider, the outcome, regardless, should be that access to the information is limited to authorized individuals only. As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA agrees that the proposed revisions support this endeavor as related to specifically configured cloud storage services; however, we observe that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions and impose new, different, and unnecessary compliance obligations on entities regardless of whether they are pursuing such options. NRECA is concerned that the way this has been	

incorporated outweighs the value of the proposed revisions relative to taking small steps toward addressing the use of could services. NRECA does not support the proposed revisions.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
We agree with MRO NSRF comments: “we believe that the proposed Requirements, by overly focusing on and prescribing technologies, will instead significantly increase administrative activities and costs as well as introduce significant new compliance risks”.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC agrees that the proposed revisions support this endeavor as related to specifically configured cloud storage services; however, observes that the proposed revisions are very limiting relative to compatibility with future or differently configured storage solutions and impose new, different, and unnecessary compliance obligations on entities regardless of whether they are pursuing such options. For this reason, GSOC is concerned that the manner in which this has been incorporated outweighs the value of the proposed revisions relative to taking small steps toward addressing the use of cloud services. As well, GSOC notes, again, that standard revisions to accommodate cloud storage are unnecessary and would be better addressed in implementation or compliance guidance. For these reasons, GSOC does not support the proposed revisions.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No

Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
No because of Part 1.5 still requires revocation of individual access privileges for third party vendors. This requires additional administrative burden for entities as they have little control over third parties. As a suggestion, the SDT could consider wording vendor access controls within “have/ implement a plan which addresses risks associated with vendor access to BCSI”	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Understand the growing use of cloud services for storage solutions, but it may be simpler to have a stand alone standard that address just cloud storage or have the applicability for just cloud services.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No

Document Name	
Comment	

The requirements should be moved to appropriate standards. The vendor requirements should be moved to CIP-013 as applicable. Part of the SCRM plan should be evaluating cloud services to meet the needs of applicable standards in scope.

R1.4 - The proposed language describes actiosn which should occur in supply chain management and should not be addressed in CIP-011.

R1.4.3 – remove the term "Mitigation Plan." This is a confusing term which connotates a regulatory mitigation plan filed w/ the ERO.

R1.4.3 – "Remediate" and "mitigate" are different actions. Please choose one or the other when using these terms

Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	
Comment	

I believe the team should consider specifying the security objectives for use of third-party storage solutions, and not limit the discussion to a risk profile similar to CIP-013. Understanding the third-party risk profile does not go far enough. When the third-party has access to an entity's BCSI, there must be a thorough understand of how the entity revents unauthorized access, manages and limits user permissions, etc. against a well-defined set of objectives.

Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	
Comment	

While the proposed requirements are a step in the right direction relative to cloud storage solutions, the language as written for Part 1.2 creates the unintended consequence of limiting the types of technology (current and future) that can be used due to the access management methods that would be necessary to implement and evidence. In support of AZPS's response to Question No. 4, AZPS believes leveraging new and future technologies would require a focus on preventing unauthorized access to identified storage locations as stated in Part 1.1, rather than a requirement to evidence

eliminating the ability to obtain and use. Alternatively, establishing a clear delineation between preventing unauthorized access to identified storage locations and the protection of BCSI during transit, use, and disposal would also provide ability to leverage different technologies.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
New and emerging technologies shift the paradigm of security controls away from a specific storage location/repository to the ability to access and use the information itself. For example, an entity that utilizes file level security can apply encrypted protections on the data that preclude unauthorized access to the data regardless of where it is stored. Requiring a list of storage locations is an antiquated construct that disincentivizes entities from using potentially more secure mechanisms because of the impossibility of compliance with documenting storage locations. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
The changes do show support and leverage towards new and future technologies but they are too specific and do not provide flexibility for the various solutions and security controls that could vary.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No

Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes proposed requirements CIP-011-3 Requirement R1, Part 1.4, and R2 Parts 2.1 and 2.2 are more likely to inhibit the use of cloud-based BCSI storage solutions than to promote it.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5 . We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic rather than stipulating a particular process or tool, such as key management.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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	
This is very similar to Question 3. Please refer to Question 3 response.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Yes, the proposed chages support future technologies but do not provide flexibility in as need.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No

Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Although the SDT is addressing the industry's request to add cloud services to store BSCI, the SDT needs to address the how to mitiage the individual terminations at third parties. It is unclear if the entities need to have an information agreement with individuals at a cloud service or with the cloud service company.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. *We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5 . We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.*	
Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
No because of individual terminations at third parties.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We appreciate the SDT's efforts to make changes that allow entities to leverage new and future technologies. We believe that the changes made here do support the concept of using cloud services; however, those changes should not impact an entity that does not use that technology. The SDT should consider that not all entities will use cloud services and should ensure that the changes do not negatively impact or create an additional burden to those entities.	
Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
No. As written, the proposed changes may not sufficiently support this endeavor much more than the existing standards. MISO proposes the following changes to provide additional clarity. As noted under our response to question 1, to more clearly articulate the key distinctions mentioned during the Q&A portion of the 2019-02: BES Cyber System Information Access Management webinar hosted on January 16, 2020, MISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows:	

"Storage locations *(physical or electronic, responsible entity or vendor hosted)* identified for housing BES Cyber System Information in the entity's information protection program"	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI member companies appreciate the efforts by the SDT to enhance Responsible Entities ability to leverage new and future technologies such as cloud-based services. However, the framework, as written, is too narrow and could potentially limit the use of future innovations and technologies that might yield better security and efficiencies.	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
NYISO feels that the proposed changes may not sufficiently support this endeavor more so than the language contained within the existing standards, NYISO offers the following suggested changes to provide additional clarity. NYISO proposes the SDT expand the language of the last example provided under requirement R1, Part 1.1, Measures as follows: "Storage locations of either physical or electronic data housed within a responsible entity's Physical Security Perimeter or housed within a vendor's hosted environment be identified as BES Cyber System Information locations as part of the entity's information protection program" NYISO understands that R1.4 and R2 attempts to cover this detail, however NYIOS feels that additional clarification is needed. NYISO's stance is that third party personnel may have physical or electronic access to encrypted BCSI, but as long as they do not have access to the keys for decrypting the BCSI, the information should be considered sufficiently protected.	
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 NextEra	
Answer	No
Document Name	
Comment	
No because of individual terminations at third parties.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
In our very the existing standard already allows. It appears NERC and FERC is not will to advertise this to entities.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
Please see response to Question 3, above. Without explicit and affirmative language, the proposed change does nothing to clarify the issue. Entities will not likely move toward cloud storage for BCSI unless CIP language specifically supports cloud storage in those terms.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	

Answer	No
Document Name	
Comment	

Alliant Energy agrees with NSRF and EEI’s comments.

While Alliant Energy appreciates the SDT’s efforts to expand information storage solutions or security technologies for responsible entities, that expansion is only useful if the requirement language is written such that it is clearly auditable. The updated requirements should avoid the ability to audit to prescriptive requirements that are not stated in the language of the requirements.

Likes 0	
Dislikes 0	
Response	

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3

Answer	No
Document Name	
Comment	

See Steven Toosevich's comments.

Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	

OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	
Comment	
Please see comments to question #3 and #6.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
There is a significant barrier in the proposed language to adoption of cloud services with regard to the EACMS definition remaining as it stands. The proposed changes do not offer entities the opportunity to make use of Managed Security Service Providers (MPPS) for their most critical systems because the systems deployed by the MSSP would still fall into the EACMS bucket. A possible solution would be to move forward with a split of the EACMS definition into EACS and EAMS, with BCSI requirements (CIP-011) applying to EAMS, and system hardening requirements (CIP-006, CIP-007, & CIP-010) applying to EACS.	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
In our view the existing standard already allows. It appears NERC and FERC is not willing to advertise this to entities.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies. We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5. We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT refers the drafting team to ERCOT's responses to Question Nos. 3 & 6.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We agree that the proposed changes address the demand to leverage new and future technologies.	

We disagee with the changes made to CIP-011 R1.3 and R1.5. This change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5. We suggest that CIP-011 R1.3 and R1.5 be changed to processes related to designated BCSI storage locations, thus maintaining the spirit of the CIP-004 access management requirements.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: No, see comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
Agree with Tennessee Valley Authority's comments about protecting access in a vendor/platform neutral manner. The focus should not be on where it is stored but how access to the documents is secured.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
The standard introduces appropriate controls for cloud storage environments. However, the standard is not specific to cloud storage and some of the items are not reasonable for internally stored information.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees that the SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Duke Energy suggests that the SDT clarify the wording of the requirements to match those of the technical rationale document. Also, the requirements as written are problematic for reasons provided in previous and subsequent responses.	
Likes 0	

Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
It is a good step forward. We need to have clarifying language for concerns previously identified.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA supports the SDT's direction; however, the language is not yet clear enough to adopt.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E believes the modifications clearly indicate that third-party providers of BCSI storage will be allowed and the objectives an entity should reach in determining the risks of the third-party usage and remediation or mitigation of those risks as determined by the entity. The non-prescriptive nature of some of the Requirement language such as "Method(s) to prevent unauthorized access" in CIP-011-3, R1, Part 1.2 could be unsettling to some entities who want to be told what needs to be done, but the objective nature provides the flexibility the SDT is trying to achieve to future proof the Standard as much as possible and not disallow technology or processes unknown to the SDT that a more prescriptive Requirement could disallow.	

As noted in Question 6, PG&E does have concerns regarding the overlap of CIP-011 R1 P1.4 with CIP-013 R1 P1.1.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	Yes
Document Name	
Comment	
The requirement is a good start towards the security methodologies needed for cloud storage.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
We are looking forward to improved wordings before answering this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

8. The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

The requirement is unclear if this is an electronic key or a physical key. This will add considerable costs to smaller entities. This is an undue burden for the industry. If you control access through an effective DMS, behind firewalls, or through the cloud processes, adding electronic key controls as prescribed by the Standard is unnecessarily burdensome for entities.

Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	

Comments: No, see comments to question 6. In addition, the key management items should be listed in the measures. Encryption should not be the only acceptable method of protecting BCSI; methods should be based on risk. Recommendation: replace "key management" with "electronic data protection methodology."

Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard. Key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implemented based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT does not believe there is a benefit to defining separate "key management" requirements. ERCOT proposes the removal of the explicit requirement and, if it is to be included at all, it should be included in the cloud vendor risk assessments considerations of Part 1.4 .

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard. Key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implemented based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

The proposed version is prescriptive overkill.

Likes 0	
Dislikes 0	

Response

Angela Gaines - Portland General Electric Co. - 1

Answer	No
Document Name	

Comment

Please see comments PGE Group 2

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	No
Document Name	
Comment	
When used in the cloud, this is integral to encrypting that data, however the use of key management by itself does nothing to protect data. Additionally, when protecting BCSI on premise, there are many alternate controls that offer significant protections without the need to use key management infrastructure.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
There is no benefit of defining separate key management requirements. Propose to remove the explicit requirement and, if at all, include in cloud vendor risk assessments considerations of R1.4.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments. Specifically, if key management is not a requirement (due to the “where applicable” language in 2.1), then it is not appropriate to have this language in the requirements section and would be better suited to guidance. The requirements should only state what is required. Additionally, it is unnecessary to require a key management program for all BCSI, which includes BCSI stored at responsible entity facilities and physical key management.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
A full and proper key management program/system is a big ask for small to medium utilities who could most benefit from cloud storage and/or managed third-party storage solutions. In this case, SNPD once again suggests, that CIP language specifically authorize a Federal IT certification as sufficient to account for proper and secure key management on the part of the certified vendor. For example, many other federal agencies use large MSSPs (Azure/AWS) to store and secure highly sensitive information without the requirement to locally control the keys. If this is sufficient for large federal agencies involved in national security, it seems that the same could be applied to BCSI. If local key management is maintained as a requirement within the proposed changes, SNPD believes many utilities will take the path of least resistance, and/or the most conservative response and simply choose to avoid cloud storage altogether – depriving utilities most in need of flexible off-prem storage the ability to realize the benefits.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
The proposed version is prescriptive overkill	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro requests that additional clarity on the definition and application of "keys" as it relates to BCSI storage locations is provided before a determination if this is integral to protecting BCSI can be made. During the NERC webinar on the proposed revisions it was indicated that keys are inclusive of encryption passwords that enable an individual to access encrypted BCSI as well as physical keys that are used to access physical BCSI storage locations; however, this is not considered sufficiently clear per the standard language.	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NextEra

Answer	No
Document Name	

Comment

1) We recommend “electronic data protection methodology” instead of “key management”.

2) We recommend moving the “key management” language to the Measures.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO feels that the requirements are too prescriptive regarding key management processes, administratively burdensome and lack a commensurate tie to what is the measurable expected outcome; i.e. a) a stated level of reliability performance, b) a reduction in a specified reliability risk (prevention), or c) a necessary competency. As noted under our response to question #6, NYISO recommends proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2 be eliminated altogether and that key management be incorporated as an example under requirement R1.

NYISO would like to see terms such as cryptographic system or cryptosystem used. If the intent is that physical keys / locks are also a part of this mandate, it should be stated explicitly. In general, encryption should not be the only acceptable method of protecting BCSI. The selected methods should be based on risk.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
EEI supports the use of “key management” for protecting BCSI at third party facilities. However, BCSI stored at responsible entity facilities are addressed in CIP-004-6 and CIP-011-2 Reliability Standards and therefore should remain an effective compliance solution with only minor modifications. The SDT should define the reliability objectives, not the method that must be used to accomplish the objective so that future technologies that might provide better protections can be used.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	

Comment
The requirements fail to state specifically when a key management program is required. The requirement in Part 2.1 starts off with, “Where applicable“, but there is no information in the proposed CIP-011-3 that provides any information on where or when it is applicable. The Technical Rationale also fails to provide any clarity on where or when a key program is needed. Also the use of term “key” by itself causes confusion on whether the requirement is referring to encryption keys or physical keys for mechanical locks. If the SDT is referring to encryption keys then they should use the term “encryption key”.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
No – as written the requirements are too prescriptive to key management processes, administratively burdensome and lack a commensurate tie to what is the measurable expected outcome; i.e. a) a stated level of reliability performance, b) a reduction in a specified reliability risk (prevention), or c) a necessary competency. As noted under our response to question 6, MISO recommends proposed CIP-011-3, requirement R2, Parts 2.1 and 2.2 be eliminated altogether and that key management be incorporated as an example under requirement R1.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should state explicitly that "Key Management" refers to encryption keys.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We agree that in today's environment, key management is widely used to support and manage the protection of information. However, our concern is that when the technology advances, these changes become "outdated" and put the industry in the same spot we are today. Whenever the opportunity arises to make changes to the standards, those changes should be risk-based and should not include a single technology solution.	
Likes 0	
Dislikes 0	
Response	

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

We recommend “electronic data protection methodology” instead of “key management”.

We recommend moving the “key management” language to the Measures.

If Key Management must be included, it should be ‘specific’, including the allowable key management options (rather than a long, and somewhat ‘vague’ list of possible controls).

Likes 0	
Dislikes 0	
Response	

Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard, key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 "develop cryptographic key process(es)." Add the term "cryptographic" as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT's intent.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment
SDG&E supports EEI's comments submitted on our behalf. Additionally, SDG&E believes there is much ambiguity in the section describing the "key management program." There should be more clarity on whether these are physical keys or software keys. The goal of this key management program needs to be clearly defined. SDG&E also seeks clarification on what items qualify to be in scope for the key management program. For example, SDG&E's Information Protection procedure accounts for unattended BCSI in transit (*e.g.*, locked vehicle, locked briefcase, etc.). Since the SDT's proposed changes are more focused on BCSI rather than the storage location, this set of proposed requirements could bring in previously undesignated/unidentified locations into scope, such as locked vehicles and locked briefcases.

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 does not agree that key management is integral to protecting unencrypted BCSI. We do agree that key management of encrypted material is integral to protecting any encrypted information. This question *assumes* all BCSI is encrypted and that **is not** the case. However, we believe the detailed prescriptive requirements in R2 may work against the goal of being able to use cloud services. For example, 8 different areas must be included in the key management program which are not discussed in the Technical Rationale document. A Google search of "Key suppression" shows no results applicable to this requirement so entities are left to guess what is meant by the words chosen in the requirement. Southern also questions why key revocation is listed twice in the same requirement part. Southern recommends that the areas of key management required are further defined and included in the Technical Rationale. Furthermore, Southern recommends that future proposed revisions of the Standard maintain the flexibility of **not requiring** encryption of BCSI when other controls can be implemented, such as access control solutions. Key management practices should be based on best practices and would be reviewed and measured as such during audit review. For Part 2.2, new terms and concepts are introduced that have no explanation, such as "BCSI Custodial entity" and their "custodial entity duties". Southern believes this requirement part is unnecessary as R1 is all about ensuring only authorized access is allowed to BCSI. Those who manage the encryption keys are required to have access to perform such management, so a non-compliance issue with 2.2 is really a non-compliance issue with R1 and Southern believes that only R1 is required to cover this risk.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic rather than stipulating a particular process or tool, such as key management.	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes cryptographic key management is necessary for electronic information but the language proposed so far causes problems for physical information storage (i.e., printed documents.)	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

R2 Applicability should be:

BES Cyber System Information stored in Vendor managed electronic BCSI Repositories, and pertaining to:

High Impact BES Cyber Systems and their associated:

1. EACMS; and

2. PACS; and

3. PCA

Medium Impact BES Cyber Systems with ERC and their associated:

1. EACMS; and

2. PACS; and

3. PCA

We recommend removing R2 from this Standard, key management should not be specified as a means, as there are others. An entity should have the flexibility to use something from their key management program as evidence of a control, without mandating specific requirements in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices. The SAR did not seek to increase required controls. Rather, it seeks language clarification around access controls and storage locations.

If R2 needs to be pursued, we recommend explicitly stating in R2.1 “develop cryptographic key process(es).” Add the term “cryptographic” as applicable within the R2 parts. Without the specificity, the Requirement could be interpreted to include both cryptographic, electronic and physical key management. We believe this was not the SDT’s intent.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST considers proposed Requirement R2, Parts 2.1 and 2.2 vastly over-prescriptive. The goal here is to ensure that no individuals who manage BCSI storage, whether in the Responsible Entity’s own data center or “in the cloud,” can access BCSI unless they have been properly authorized in accordance with the requirements of CIP-004. Encryption and key management are certainly viable options, but they should remain options. N&ST suggests moving them to the “Measures” associated with an appropriately re-worded requirement.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3
Answer	No
Document Name	
Comment
Managing keys does play an important role for protecting BCSI but in order to fully utilize new technology, key management cannot be the sole focus. It is important to ensure there are other layered security measures in place to allow for flexibility with keys. Not all new and future technologies can be implemented with such restricted key management requirements. Instead, we recommend the requirements be converted to objective-based requirements by removing “which shall include the following: 2.1.1-2.1.9.”
Likes 0	
Dislikes 0	
Response
Vivian Moser - APS - Arizona Public Service Co. - 3
Answer	No
Document Name	
Comment
AZPS does not agree that the proposed requirement to implement a key management program is integral to protecting BCSI. The addition of a requirement for a specific access control method (i.e., a key management program) is too prescriptive. AZPS recommends the same approach as discussed in previous comments above, wherein the focus remains on the protection of BCSI, rather than requiring specific controls. AZPS believes that Entities are well-positioned to assess and implement access control methods best suited to protect their BCSI. The Technical Rationale for CIP-011-3 states that a key management program provides an extra “layer of defense against bad actors who may have the means to physically or electronically obtain BCSI but not use or modify BCSI but not use or modify BCSI”. AZPS does not believe that the risk associated with obtaining BCSI but not being able to use or modify BCSI does not support implementation of a key management program.
Likes 0	
Dislikes 0	
Response
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5
Answer	No
Document Name	
Comment

No. Please see response to Q6. Key management is a possible measure for preventing unauthorized access, not an independent requirement.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Key management should be a requirement for off-site storage of BCSI or BCSI in the cloud.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We recommend “electronic data protection methodology” instead of “key management” which is too prescriptive
We recommend moving the “key management” language to the Measures
We would prefer the “If Applicable” to include language that says this is mandatory only if you are using encryption or encrypted protocols

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC agrees with comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

If selected as the security control to for access to BCSI, then, encryption is integral to protecting BCSI. However, encryption is not the only method or security control to the overall protection of BCSI. The focus of the “key management” requirements that were added to CIP-011, while helpful where encryption is utilized, are somewhat limiting to and leave unaddressed other methods and security controls that could be employed to protect BCSI. Further, use of the term “key” could create confusion and ambiguity regarding the scope of these requirements, e.g., does it address electronic and physical key management or merely electronic key management. Finally, GSOC is concerned that, as written, these new requirements may not be flexible enough to maintain applicability #3 technology changes and evolves. Please refer to GSOC’s response to question for additional comments regarding the limited applicability of these newly proposed requirements.

Additionally, GSOC notes that “custodial entity” is an undefined term and, therefore, could be interpreted broadly and variably. Further, there is not a clear indication of where or how the “controls” would be documented and maintained. This is significant as it interpretations of how to demonstrate compliance during compliance monitoring could vary across entities during implementation and across regions and audit teams, resulting in inconsistency in enforcement. As well, the use of the term “methods” within the measures has the potential to further complicate implementation and interpretation.

Finally, GSOC is concerned that a single control failure would result in a violation of requirement R2.2 regardless of whether other controls existed and duties remained separated. GSOC respectfully asserts that such ambiguity places auditors and Responsible Entities in uncertain and tenuous positions that would likely cause both to militate toward conservatism, resulting in over-reporting and -enforcement. For these reasons, GSOC requests that the SDT provide clarification of the term “custodial entity,” the expected compliance documentation, and the overall compliance obligation to avoid unnecessary compliance activities and risk.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

R2 Parts 2.1 and 2.2 exceed the scope of the SAR and significantly increase the compliance obligations. CIP-011 should remain non-prescriptive and allow entities to implement the controls appropriate to their situations, which could be something other than encryption and key management. An entity is free to use something from their key management program if they have one to use as evidence of a control, without mandating specific requirements

in the standard. The ERO Enterprise CMEP Practice Guide: BES Cyber System Information dated April 26, 2019 suggests auditors review whether key management practices were implement based on best practices.

It is also unclear as to what “where applicable” means, and whether this requirement applies to physical keys and passwords to on premises systems.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

If selected as the security control for access to BCSI, then, encryption is integral to protecting BCSI. However, encryption is not the only method or security control to the overall protection of BCSI. The focus of the “key management” requirements that were added to CIP-011, while helpful where encryption is utilized, are somewhat limiting to and leave unaddressed other methods and security controls that could be employed to protect BCSI. Further, use of the term “key” could create confusion and ambiguity regarding the scope of these requirements, e.g., does it address electronic and physical key management or merely electronic key management.

Additionally, NRECA notes that “custodial entity” is an undefined term and, therefore, could be interpreted broadly and variably. Further, there is not a clear indication of where or how the “controls” would be documented and maintained. This is significant as interpretations of how to demonstrate compliance during compliance monitoring could vary across entities during implementation and across regions and audit teams, resulting in inconsistent enforcement. As well, the use of the term “methods” within the measures has the potential to further complicate implementation and interpretation.

Finally, NRECA is concerned that a single control failure would result in a violation of requirement R2.2 regardless of whether other controls existed, and duties remained separated. NRECA believes such ambiguity places auditors and Responsible Entities in uncertain and tenuous positions that would likely result in over-reporting and -enforcement. NRECA requests that the SDT provide clarification of the term “custodial entity,” the expected compliance documentation, and the overall compliance obligation to avoid unnecessary compliance activities and risk.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	

Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP is of the opinion that key management methods can be either partially accessible or not accessible at all in certain cloud storage environments, which could increase security risks associated with the protection of BCSI. We also feel it is unnecessary to develop a key management process for the storage of BCSI within a Responsible Entity's own facility, but without more clarification surrounding the "where applicable" language, we are unsure if the language is specifically addressing third party storage locations or BCSI storage as a whole.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
While Black Hills does agree that key management is crucial and appreciates it addition, we think further clarification should be added for information held by a provider or third-party. If the intent is for on-premis items as well, we think that key management should be listed as an example of possible controls and not the sole means.	
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	
As such, suggest re-architect the standard to be outcome based so as not to preclude using specific technologies or adoption of emergent solutions. As such, geo-location or biometric protections are not available as options to RE's.	

Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We support NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Managing keys does play an important role for protecting BCSI but in order to fully utilize new technology, key management cannot be the sole focus. It is important to ensure there are other layered security measures in place to allow for flexibility with keys. Not all new and future technologies can be implemented with such restricted key management requirements. Instead, Tri-State recommends the requirements be converted to objective-based requirements by removing “which shall include the following: 2.1.1-2.1.9.”	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Although key management can be an effective control and a good security practice, it is not integral to protecting BCSI in all cases. Focusing attention on this one type of control once again ties the Standard to a specific technology concept that 1) is not applicable in all cases, 2) may become obsolete in part or in whole from unexpected technological developments, and 3) stifles alternative and creative approaches to security. Seattle believes key	

management should NOT be a specific requirement of the revised CIP-011, but it should be identified in the Measures and discussed in detail in the guidance documents as one effective approach that can be applied in many (but not all) situations.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Agree with the proposing a new “key management” set of requirements, but need clarification for the written language in R2 (See our response in Question 6).	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Key management should not be specified as the means; Entities should be free to pursue any means that achieves the objective. We believe protecting BCSI is best handled in the CIP-004 Access Control Requirements. R2 Part 2.1 should be deleted in its entirety.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Including a key management requirement may burden entities who do not have a key managmenet infrastructure. The requirement also requires encryption as a technology that some entities may not want to employ.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

We believe that this requirement is currently not adequately defined. The requirement language implies that this refers to encryption key management, but the technical rationale includes a physical component. It is not a trivial task to encrypt ALL BCSI, so please clarify that a key management program is not required for situations where BCSI is protected via another means. The technical guidance contains only two paragraphs for a key management program with nine management requirements. Please include technical examples that would suitable comply with each of the nine key management activities.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

This question is ambiguos and need more clarity. "key managment" ? Proposed language is not sufficient. Stating no here to insure other concerns are addressed.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree with the new “key management” set of requirements. Duke Energy would like clarification if key management applies to electronic keys only and not physical keys. It is unclear what constitutes a custodial entity. It ignores other options for securing physical BCSI (e.g. badged access), and other forms of physical controls that could be used for access to physical BCSI.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No

Document Name	
Comment	
The standard is appropriate for externally stored information under the direct control of the entity such as in a cloud environment. However, two cases where this is unreasonable: (1) Information stored by a consulting partner under non-disclosure agreement on systems owned and operated by a consulting partner. (2) Information stored internally on entity owned systems where the company has chosen to perform encryption for other reasons. I would not look forward to maintaining a key management program on each Microsoft Windows computer protected with BitDefender.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
This represents a large burden on smaller utilities and those who outsource support.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the addition of key management will be critical to the protection of BCSI not only in third-party environments, but also for internal usage to protect BCSI. Key management will demonstrate to Audit Teams the entity has the BCSI protected, and a lack of key management will raise serious concerns on how the BCSI is being protected. As noted in Question 6, PG&E recommends the requirement language clearly indicate key management covers the physical and electronic types of keys.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

While “key management” is one way to effectively protect BCSI, this is too prescriptive in dictating “how” to comply, and therefore not future proof. The requirement should be technology agnostic and objective based, so it is written to focus on the implementation of effective methods that afford adequate security protections to prevent unauthorized access to the information, so it is scalable and does not preclude use of new and emerging technologies as they become available.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	Yes
Document Name	

Comment

R2. - Encryption of BCSI and key management is the only potential method for entities to be able to utilize cloud services yet control CIA of data. It is imperative that access control include encryption as a method to prevent access

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

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	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	

No comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

9. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree that to the significant change of focus to BCSI from BCSI designated storage locations, additional controls, compliance processes, and evidentiary documentation at a significant cost would be required along with requiring significant efforts of a technical, administrative, and operational nature to meet the new Requirements.

CIP-011-3, R1, Part 1.3 - "focus changed from access to designated storage locations to access to BES Cyber System Information" It is not clearly defined what information, independently or collectively, establishes the designation of BES CSI. The review and management of current designated storage locations (and data) are managed by designated employees. The requirement that all potential BES CSI is guarded in transit and use increases the number of individuals requiring training and potential access to the repository. An independent host name or IP address, independently, is not currently labeled BES CSI. An individual without NERC privileges may have that information for daily work at a Generation station.

CIP-011-3, R1, Part 1.6 - "focus of verification changed from designated storage locations to BES Cyber System Information: It is not clearly defined what information, independently or collectively, establishes the designation of BES CSI. An independent host name or IP address, independently, is not currently labeled BES CSI. It is not possible for a small subset of individuals to review and manage all data throughout generation stations that 'may be' considered BES CSI based on an unclear definition.

CIP-011-3, R1 Part 1.5 "focus of termination actions changed from access to designated storage location to access to BES Cyber System Information". This is not feasible in the case of individuals access to documentation that is considered "in use" such as hard copies of information. It is not feasible to manage at the document level while removing access from repositories can occur electronically and instantly.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

As written, this will have the opposite impact due to the focus on the lifecycle of BCSI. Any BCSI that is stored and transmitted by BCS, EACMS, PACS, or PCAs will now require specific protections. For example, BCSI stored in ourBCS will now need to have extra protections during storage and transit between BCS ad associated assets above what is required for operation for the BCS. This is not itself a bad thing, but as written this will be required by the proposed changes.

Likes 0	
Dislikes 0	

Response
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller
Answer	No
Document Name	
Comment
Needs further discussion and clarification.
Likes 0	
Dislikes 0	
Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino
Answer	No
Document Name	
Comment
Specifically focusing on storage locations defined what to protect. Entities may not know the location of BES CSI at all times when in use and transit.
Likes 0	
Dislikes 0	
Response
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF
Answer	No
Document Name	
Comment
The approach will significantly increase unnecessary controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on identified storage locations. If the intent is to shift the focus to the BCSI rather than storage locations, why is there a requirement to list storage locations (R1 Part 1.1)? See also comments to question 1. Not sure what is meant by unneeded controls on BCS.

As to the concept itself, we believe it will be more difficult to apply requirements to BCSI than the assets or storage locations in which it resides, and therefore are resistant to this approach. Better to define BCSI Repositories and BCSI Access per previous responses.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Disgree with eliminating BCSI storage locations. If the intent is to shift the focus to the BCSI rather than storage locations, why is there a requirement to list storage locations (R1 Part 1.1)? We believe BCSI Repository identification (see our response in Question 1) is centric for preventing unauthorized	

access to the BCSI in that it is difficult to apply requirements to BCSI than the assets or storage locations in which it resides. For example, if a person wants to have an authorized access to BCSI, he (she) should request access to the BCSI respository first. This approach ensures the person who possess the BCSI will always has authorized access to the BCSI. The BCSI Repository and BCSI requirements should be working together to prevent unauthorized access to BCSI.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is concerned that this proposed approach reopens the challenges of protecting individual “pieces” of BCSI that plagued CIP v1-3, adds complexity, and introduces unintended consequences. This change ultimately MIGHT be the most effective one, but it should be vetted and explored and explained in much more detail to minimize perverse outcomes.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State understands and agrees with the intent, however, as currently drafted, applicability and how to comply with the requirements become blurred. For example, if the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.

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	
This increases a entities controls that are needed for BCSI. An entity would have to defined multiple process elements to further define and control BCSI while it is in flight or in all storage locations that could have BCSI.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not agree that this approach reduces potential unneeded controls on BCS. Additional BCSI related requirements feel unnecessary, and we feel making modifications to access control requirements could address this issue.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	

Answer	No
Document Name	
Comment	
While this approach may reduce the potential for unnecessary controls on BCS, it introduces significant other compliance activities/obligations and required security controls with which Responsible Entities must comply. Accordingly, the revised approach does not achieve a net reduction in effort or scope of security controls and – likely – results in an increase of same without any resulting increase in security or reliability.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
While we agree with the approach, the draft does not accomplish this. The focus can be shifted to the BCSI itself to meet the goals of the SAR by slightly modifying CIP-004 R4, Part 1.4.3 to [Process to authorize. . .] “Access to BES Cyber System Information in designated storage locations.” The focus of CIP-011 has always been on the BCSI, so we contend that the changes proposed in R3 directly contradict this by changing the focus to the assets and storage media, rather than the BCSI.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
While this approach may reduce the potential for unnecessary controls on BCS, it introduces significant other compliance activities/obligations and required security controls with which Responsible Entities must comply. Accordingly, the revised approach does not achieve a net reduction in effort or scope of security controls and – likely – results in an increase of same without any attendant increase in security or reliability.	
Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The proposed changes do not reduce potential uneeded controls on BCSI it adds more controls.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
I do not believe this will lessen the controls as security will still be needed for the physical locations as well. Further, the proposed standard provides greater specificity in R1 Part 1.1 in identifying BCSI storage locations.	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
Although AZPS agrees that the proposed requirements reflect an intent to increase security controls to protect BCSI, protection through management of access to storage locations should remain separate from protection of BCSI in transit, use, and disposal.	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State G&T understands and agrees with the intent, however, as currently drafted, applicability and how to comply with the requirements become blurred. For example, if the requirements are kept focused on designated storage locations for BCSI, it eliminates confusion with BCSI that may reside in BCS, EACMS and PACS. We understand that this is a challenging part of the project, but we are concerned that the applicability and associated requirements as currently drafted will create confusion, redundancy and expanded scope. Other than reverting back to the original structure, a possible solution could be to add exclusions to the applicability to exclude High and Medium Impact BCS and their associated EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST is curious to know what “potential unneeded controls on BCS” might be reduced by changing the existing requirement to manage access to BCSI storage locations to a requirement to grant, review, and revoke access to BCSI itself. In any case, N&ST believes such a change would have the potential to significantly increase a Responsible Entity’s access management program workload and significantly increase its compliance risk (how would an Entity convincingly demonstrate revocation of access to BCSI had been accomplished within the prescribed time frame?), with little or no reduction of risk to BES Cyber Systems and the BES. N&ST believes the existing requirements of CIP-011 implicitly but adequately convey an obligation to ensure BCSI cannot be accessed by unauthorized individuals.

N&ST strongly opposes this proposed change.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.

The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only ads significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA finds the strategy is reasonable but implementation of the exact verbiage needs care. Various cyber security methodologies often address cyber system protection strategies and information protection strategies separately. It's also necessary to address the Cyber Asset definition where it includes "data in the device" to clarify and make the language consistent. Potential conflict between proposed requirements for protecting system data vs requirements protecting systems/devices would be very bad. The positive side of protecting the information rather than the storage location is that specific controls for digital information such as encryption come into scope and these methods are very effective when properly implemented. The SDT must continue to consider the physical storage of printed materials as well so as not to exclude the possibility of protecting physical storage locations under some facsimile of the current methodology.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. Physical locations may require a different approach from cloud based storage of BCSI data.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	

Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
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 agrees that certain hardware/device/Cyber Asset level requirements (such as CIP-011 R2) must change in order to allow for cloud services. However, Southern does not agree that a wholesale move to protecting BCSI rather than BCSI storage locations is measurable or auditable as per our answer to Question 2. In essence, Southern agrees that the focus needs to change from BCSI physical or hardware storage locations. However, “BCSI storage location” does not necessarily imply physical or hardware issues, it can just as easily point to a dedicated and protected area within a cloud service offering. CIP-011-1’s current R2 needs to be updated so that it is **not** Cyber Asset and physical media based, however in this proposal it remains as such.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
See response in question #6 and #7.	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf. Additionally, for proposed CIP-011-3 R3.1, SDG&E suggests the draft retain the language "…that contain BES Cyber System information…" Otherwise there is a requirement to sanitize assets which may not contain BCSI and may not have an available method for sanitization.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.	

The approach will significantly increase controls on BCSI by eliminating the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only ads significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations).

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
There is no opportunity in the proposed standards to reduce controls on BCS, rather the proposed changes represent a vast increase in required security controls and evidence gathering obligations.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support additional Requirements to BCSI. Instead, the recommendations contained within our response to Question 4 could provide an equally effective solution resulting in fewer changes to existing processes for responsible entities. In addition, the inclusion of the undefined term of “storage locations” may create new obligations for entities who desire to use third party storage locations. This would necessitate that entities continue to identify and protect the physical location and hardware of host repositories. This may keep industry from using cloud-based services. As an alternative, the requirements could be written to only require entities to identify the repository name, type of repository (electronic or physical) and identifying if the repository is managed onsite by the responsible entity or offsite by a third party.	
Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
I would agree if that were the approach; and if this proposal was not so prescriptive; and if this proposal was not so way out to the SAR scope.	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
We agree with the approach however the language in the requirement does not achieve this goal. If the desire is to securely handle the information itself, SNPD suggests a mandatory labelling and protection scheme akin to DoD requirements for protection of classified data. Requirements are clear, implementation is simple, and accountability is baked in.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	

Answer	No
Document Name	
Comment	
The definition of storage locations needs to include references to physical protections. A shift away from physical protections or 'hardware' dilutes the concept of security around BCSI.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
See comments for Part 1.1. Shifting the emphasis away from where the information is stored will increase potential unneeded controls for BCSI. Rather than focusing on the systematic protection of those locations where controls can be applied, the revisions can be seen as requiring protection of individual pieces of information. This would be tremendously burdensome and possibly unattainable.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	

Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I would agree if that were the approach; and if this proposal was not so prescriptive; and if it was not so way out of the SAR scope.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations. The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information. We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only adds significant burdens and impossible evidentiary requirements.	
Likes 0	
Dislikes 0	

Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT refers to its comments concerning Part 1.1., and believes that shifting the emphasis away from where the information is stored will increase the potential of unneeded controls for BCSI. Rather than focusing on the systematic protection of those locations where controls can be applied, the revisions can be seen as requiring protection of individual pieces of information. Requiring protection of individual pieces of information would be tremendously burdensome and possibly unattainable.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We are concerned with this approach. Authorizing access to BCSI is problematic unless the access requirements and controls are specific to the designated BCSI storage locations.

The approach will significantly increase controls on BCSI by eliminating the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems, and adding authorization/revocation and review requirements for all BCSI, instead of only on designated storage locations. As stated previously, there is no benefit to these additions because without ERC, a bad player would not be able to remotely access and use the information.

We believe that focusing on access controls to storage locations adequately address the risks. A shift of focus to the BCSI rather than storage locations is unnecessary and only adds significant burdens and impossible evidentiary requirements.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

It is agreed that the focus should be on protecting the BCSI and Responsible Entities should have the flexibility to build a program that best fits their needs. These revisions seem to focus mostly on encrypting data, which is a good component of a bigger program; however, if it is a requirement to encrypt data, it can hamper the Responsible Entity’s flexibility to develop a program that meets its needs in a variety of situations.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The location where BCSI is stored is too difficult to separate from the BCSI itself. The requirements should remain focused on the storage location with the addition of key management for third party storage locations.

Likes 0	

Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The SDT appears to have made this more convoluted and burdensome by prescribing key controls and other methods.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Agree that this is the correct approach. Greater clarity is needed within the requirements to place the requirements in the appropriate context and prevent a default fallback to the prior interpretation in the requirements.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: If this is in fact the intent of the SDT, then why is the SDT including a risk assessment of 3rd party storage solution providers? An RE would just be leveraging the 3rd party storage solution provider's hardware (physical or virtual) for a storage location.	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
However, we wish for clarity on this question.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills agrees that focusing on the protection of the information rather than simply access to it is a better approach	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
If this is in fact the intent of the SDT, then why is the SDT including a risk assessment of 3rd party storage solution providers? An RE would just be leveraging the 3rd party storage solution provider's hardware (physical or virtual) for a storage location.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations)	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
recommend focusing on protecting data (CIA)	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
While there is agreement to focus the security on the BCSI making the answer to the question asked a “Yes” the presence of “storage locations” in Requirement R1 defeats this SDT intention. Therefore, in its proposed form the requirement language neither aligns with nor accomplishes this stated objective	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	Yes
Document Name	
Comment	
We agree with the approach to shift the focus of security to the BCSI; however, the SDT should consider their execution of the approach as described above.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Yes – completely agree.	
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 NextEra	
Answer	Yes
Document Name	
Comment	
We agree with this approach but we believe this update is not backwards compatible (primarily because of the new Applicability / storage locations).	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment
OPG is in agreement with RSC provided comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike

Answer	Yes
Document Name	

Comment
However, the SDT has not completed this process in updating the previous R2, now R3 controls. Prescribing sanitization or destruction controls eliminates the ability to use encryption to restrict unauthorized access, which is a viable control. We suggest moving this back to the Objective level of preventing unauthorized access to... Or leverage the updated 1.2 language of: "Method(s) to prevent unauthorized access to BES Cyber System Information by restricting the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal, to authorized access holders." Which explicitly includes storage and disposal (and possibly eliminate R3 entirely).

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment
PG&E agrees with the shift to “System Information” (i.e. BCSI) and away from the security of the hardware. The Standard should be about Cyber Asset information and not the Cyber Assets themselves.

Likes 0	
Dislikes 0	

Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Comments: The SDT should review all the requirements to ensure that new or updated requirements do not have the unintended consequence of hindering an Entity's ability to store or use BCSI in the Cloud. See comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that the changes align better with the purpose of CIP-011, which reads, “To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).” Texas RE does, however, recommend the SDT consider language to permit the use of third party equipment without also removing all security obligations from equipment owned and maintained by Registered Entities since the SDT’s goal is to allow BCSI storage in equipment not owned or managed by Registered Entities (e.g. cloud providers).	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

10. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

Comments: While this supports separation of controls associated with information as opposed to cyber assets/systems, it also separates controls related to access management into two standards, which may impact an entity's program organization breakdown (i.e. central approaches to access management now dealing with two standards instead of one). It would be preferable to have the access authorization/revocation requirements to be centrally located in CIP-004. Related CIP-004 requirements should sufficiently cover concerns about individual terminations at third parties.

Likes 0	
Dislikes 0	

Response

Colleen Campbell - AES - Indianapolis Power and Light Co. - 3

Answer	No
Document Name	

Comment

The CIP-004 requirements concerning BCSI revolve around authorized access to the information, that should remain in CIP-004 to maintain consistency with the current requirements and the data already collected.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

No, It is not agreed this approach provides greater clarity; rather, this approach introduces and creates ambiguity. The authorization, revocation, and review requirements should remain in CIP-004. By consolidating requirements for BCSI, the SDT is separating authorization, revocation, and review

requirements. It is better to keep the BCSI protection controls in CIP-011 and the authorization, revocation, and review requirements in CIP-004 as those are more programmatic in many cases to an organization.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding “with ERC” for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment
ERCOT agrees with the rationale provided regarding treating BCSI differently than Cyber Assets. However, ERCOT believes the changes would be more appropriately made by adding new parts to CIP-004, Requirements R4 and R5 that address the unique needs of BCSI. This would avoid the existence of “spaghetti requirements” and unwanted side effects of cross referencing requirements. In versions 1-3, the access requirements for BCSI were included in CIP-003. Industry provided strong feedback suggesting all access requirements should be in one location, which is why the requirements were added to CIP-004. There are entities that use a consolidated access management program to meet all regulatory requirements. Having all requirements in one location helps support this type of program. An alternative approach would be to separate the BCSI requirements into separate rows in their respective requirements of CIP-004, Requirement R4 and R5. ERCOT suggests the drafting team Consider revising Part 4.1.3 into a separate row within the CIP-004, Requirement R4 table. ERCOT believes the requirement language as written in CIP-004-6 should be retained to focus on where the information is located.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding “with ERC” for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
Access requirements should remain in CIP-004.

Likes 0	

Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	No
Document Name	
Comment	
Please see comments PGE Group 2	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	No
Document Name	
Comment	
PGE agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Agree with the rationale provided of treating the BCSI different than Cyber Assets. However, the changes would be more appropriately made by adding new parts to CIP-004 R4 and R5 to address the unique needs of BCSI. This avoids the existence of "spaghetti requirements" with unwanted side effects of cross referencing requirements. In versions 1-3, the access requirements for BCSI were included in CIP-003. Industry provided strong feedback wanting all access requirements in one location, so the requirements were added to CIP-004. There are entities that use a consolidated access management program to meet all regulatory requirements. Having all requirements in one location helps support this.	

An alternate approach is to separate the BCSI requirements into separate rows in their respective requirements of CIP-004 R4 and R5. Consider making 4.1.3 into a separate row within the CIP-004 R4 table. The requirement language as written in CIP-004-6 should be retained to focus on where the information is located.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	No
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

It would be more beneficial to maintain all access requirements under one Standard. Keeping access management and review programs and procedures under one Standard would reduce any confusion and decrease margins for error with compliance obligations and good sound security practices. A holistic security standard would include requirements for access approvals, revocation, and annual reviews, which is greatly important if the same department is responsible for those requirements.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant Energy agrees with NSRF and EEI's comments.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

Access requirements should remain in CIP-004.

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 NextEra

Answer	No
Document Name	

Comment

1) No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party's staff leaves.

2) Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person's access?

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

NYISO recognizes and agrees with the SDT's intent to consolidate similar issues. We recommend that the SDT pursue the maintenance of all personnel and access management requirements be contained within CIP-004-7 to better align with existing industry practices. As noted in our response to question #2, our concern with introducing access management requirements under CIP-011-3 is that it introduces a new complication, that of having to maintain similar access authorization, revocation and control measures that are currently mandated within CIP-004-7. NYISO would see this as requiring a responsible entity to be maintaining access management controls in support of two separate standards (i.e. CIP-004-7 for BCS and CIP-011-3 for BCSI), there is the potential for a single deficiency in an entity's access management program to result in non-compliance with two different NERC standards.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Please note EEI comments to questions 8 and 9 above.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	
Comment	
No. Although MISO recognizes and agrees with the SDT's intent to consolidate similar issues. We recommend that the SDT maintain all personnel and access management requirements within CIP-004-7 to better align with existing industry practices. As noted in our response to question 2, our concern with introducing access management requirements under CIP-011-3 is that it introduces a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. By having to maintain access management controls in support of two standards (i.e. CIP-004-7 for BCS and CIP-011-3 for BCSI), there is the potential for a single deficiency in an entity's access management program to result in non-compliance with two NERC standards.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The standards development team should support specific requirements providing appropriate levels of security for Cloud Service Providers and 3rd Party Access. Transferring the CIP-004 BCSI requirements to CIP-011 does not address the unique issues created by storing BCSI in repositories that are not controlled by registered entities. The standards development team should draft separate requirements.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support MRO comments.	
Likes 0	
Dislikes 0	
Response	

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
We believe that this could complicate CIP access management programs. These changes seem contrary to the work completed by the V5 project team to remove the “spaghetti” requirements.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party’s staff leaves. Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person’s access?	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding "with ERC", for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties. It is problematic for the Entity to know when a third party's staff leaves Part 1.5 does not addess a) when the BCSI was given to the vendor and b) how to revoke one person's access?	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	

Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Moving BCSI access revocation requiment from CIP-004 to CIP-011 can resulting in multiple violation of a single instance.	
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 does not agree that this provides greater clarity, as it loses context. For example, the proposed R1.5 is pulled out of its CIP-004 context where it was one of five parts of an access revocation program requirement. It is then inserted into CIP-011 with no context. Read in a vacuum without the CIP-004 "Personnel and Training" standard context, Part 1.5 suddenly mentions "the individual" and "termination actions". What do those mean outside of the CIP-004 context? The requirement part prior to this was discussing vendors, so does this apply only when you terminate a vendor? Southern strongly suggests leaving the CIP-004 personnel and access management issues within CIP-004 so they don't lose vital context in a transition to CIP-011.	
Likes 0	
Dislikes 0	

Response
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC
Answer	No
Document Name	
Comment
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES
Likes 0	
Dislikes 0	
Response
David Jendras - Ameren - Ameren Services - 3
Answer	No
Document Name	
Comment
Ameren agrees with and supports EEI comments.
Likes 0	
Dislikes 0	
Response
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion
Answer	No
Document Name	
Comment
Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The current approach taken by the SDT appears too proscriptive and should remain flexiable and technology agnostic.
Likes 0	
Dislikes 0	
Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA finds the strategy is reasonable but implementation of the exact verbiage needs care. Various cyber security methodologies often address cyber system protection strategies and information protection strategies separately. It's also necessary to address the BCS/BCA definition where it includes "data in the device" to clarify and make the language consistent. There could be impact on CIP-010 for change (configuration) management as the distinction between "data" and "software" is blurry in some cases. Certain best-practice managed-configuration items often referred to as "settings" (user configured inputs to the runtime parameters of a software application or operating system) that drastically affect the operation of the system are not tracked in CIP-010. These configuration items are "data in the device required for its operation" and also present an item of interest to the malicious actor and a reliability issue if they are inadvertently altered; even such things as Internet Protocol addresses and subnet masks, hostnames, Domain Name System (DNS) entries, Network Time Protocol (NTP) server addresses and similar parameters that enable reliability of a system and are not considered in CIP-010 but are covered by the current understanding of BCSI. Potential conflict between proposed requirements for protecting system data vs requirements protecting systems/devices would be very bad.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

We do not agree that this provides greater clarity between BCSI and BCS requirements. The difference in Medium Impact applicability needs to be addressed by adding "with ERC", for the access requirements in R1.3 and R1.5 and these requirements need to be limited to designated storage locations of BCSI.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST sees no benefit in moving BCSI storage location access requirements from CIP-004 to CIP-011 and believes there is no need for clarification between BCSI and BCS requirements. Furthermore, N&ST believes that the impact of moving some access management requirements from CIP-004 to CIP-011 could be significant for some Responsible Entities, compelling needless modification and disruption of mature and effective CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

While there is appreciation for the desire to “group” requirements by “applicable system”, this change fosters a bifurcated model for user and access management instead of incentivizing an enterprise program to manage risks and provisioning/deprovisioning tasks that can be unplanned and considered high frequency security operations. The SDT should resist the temptation to revert back to previously problematic constructs that created “spaghetti” in the Requirements, and maintain the construct that groups access management as a business process collectively under CIP-004. Access to BCSI also not just 3rd party and to move these requirements out from under the umbrella of user and access management in CIP-004 seems like a step backwards

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	No
Document Name	
Comment	
AZPS does not necessarily agree that that the transfer of BCSI-related requirements from CIP-004 to CIP-011 provides greater clarity; however, is not opposed to aggregating all BCSI-related requirements into one standard.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
The standard does not consider nor add clarity to the third-party access and revocation requirements, a gap in security objectives as discussed in the response to Q7.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Access management is access management keep it in CIP-004. CIP-004 includes physical and electronic access to BES Cyber Systems and BCSI. It needs to remain together. Implementing this change would cause industry to ramp-up many internal governance process changes to meet this proposed change	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	

Answer	No
Document Name	
Comment	
No, the current version of CIP-004 already provides for the identification of BCSI storage locations. Keeping all the requirements for access and revocation in one standard decreases the complexity for compliance.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
No because Part 1.5 will require individual terminations at third parties and does not address a) when the BCSI was given to the vendor and b) how to revoke one person's access?. See our comment to Question 7 While we understand the difficulty the SDT faces with leaving BCSI access requirements in CIP-004, we would prefer that all access requirements remain together within CIP-004	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No

Document Name	

Comment

No. First, GSOC respectfully suggests that the removal of requirements from CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6 and the addition of these requirements to CIP-011-2. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

Second, there is significant value in the consolidation of access management requirements in 1 standard. For example, the ability of Responsible Entities to apply consolidated processes, to better ensure that minimal impacts occur as a result of revisions to standards or processes, to leverage similar or the same compliance documentation, etc. Moving only a portion of Responsible Entity's access management requirements from CIP-004 to CIP-011 places access management obligations in multiple standards, eliminated current synergies, creating confusion and process inefficiency, and increasing compliance risk. It also likely results in the requirement to modify multiple standards where access management of system scope revisions are proposed – instead of being able to implement revisions in just one standard, creating more work for SDTs and increased monitoring and commenting effort by industry.

Finally, GSOC fails to see the reliability value in segregating these requirements into 2 standards. As well, the benefits listed in the Technical Rationale are not reliability benefits, but are, rather, administrative improvements. This is highlighted by the shift to BCSI instead of locations as this shift has the likely effect of expanding access to BCSI beyond what is actually needed by personnel, exposing more BCSI to the risk of unauthorized access. For these reasons, GSOC does not support the relocation of the CIP-004 requirements associated with BCSI to CIP-011.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

We commend the SDT for trying to consolidate all BCSI-related requirements. However, we believe CIP-004 remains the more appropriate place for the access management requirements because 1) that is where other access management requirements are located, and entities have created their access management programs based upon this, and 2) having access management requirements in two places creates the potential for multiple violations for one instance (see MRO NSRF comment).

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

No. NRECA believes that the removal of requirements from CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6 and the addition of these requirements to CIP-011-2. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

Additionally, there is significant value in the consolidation of access management requirements in a single standard. For example, the ability of Responsible Entities to apply consolidated processes, to better ensure that minimal impacts occur because of revisions to standards or processes, to leverage similar or the same compliance documentation, etc. Moving only a portion of Responsible Entity's access management requirements from CIP-004 to CIP-011 places access management obligations in multiple standards, eliminates current synergies, creates confusion and process inefficiencies, and increases compliance risk. It also likely results in the requirement to modify multiple standards where access management of system scope revisions are proposed – instead of being able to implement revisions in just one standard, creating more work for SDTs and increased monitoring and commenting effort by industry.

Finally, NRECA fails to see the reliability value in segregating these requirements into 2 standards. As well, the benefits listed in the Technical Rationale are not reliability benefits, but are, rather, administrative improvements. This is highlighted by the shift to BCSI instead of locations as this shift has the likely effect of expanding access to BCSI beyond what is needed by personnel, exposing more BCSI to the risk of unauthorized access. NRECA does not support the relocation of the CIP-004 requirements associated with BCSI to CIP-011.

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	

AECI supports comments filed by NRECA

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	
Fragmenting user access across two standards is a regressive action that negates a substantive uplift that NERC adopted in the version 5 standards. Suggest retain all user access controls in CIP-004.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
If specific access controls are deemed necessary, Seattle prefers that access requirements remain grouped in CIP-004, and furthermore recommends alignment of termination timing for BCSI from “calendar day” to “24 hours” as is consistent with timing for other termination requirements. Even better to Seattle would be to drop specific access requirements for BCSI and/or BCSI storage locations from either of CIP-004 or CIP-011, and left up to each entity to specify in their risk-based BCSI security plan. Expectations and guidance could be provided in the Measures and technical documents.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3 (see our response in Question 2) and we havn’t seen any security needs for this change.	
Likes 0	

Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
This places access management outside of CIP-004.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Not until the difference in Medium Impact applicability is addressed (add “with ERC”), and these requirements are limited to designated storage locations of BES CSI.

Per our response to Question 2, we disagree with moving requirements for access to BCSI from CIP-004-6 to CIP-011-3. We appreciate the attempt to streamline Requirements associated with BCSI by placing all related compliance activities solely within the CIP-011-3 Standard. However, by doing so Responsible Entities would be subject to the potential of having multiple compliance issues with one failed compliance activity as a result of the overlapping NERC CIP Standards.

To describe the scenario we offer the following: If an Entity were to have an employee, contractor or vendor with approved access to BCSI and no other physical or logical access to BES Cyber Systems or Cyber Assets and that employee left the company then we would be required to revoke access by the end of the next calendar day, per CIP-011-3 R1.5. If we were to have a miss and not revoke by the next calendar day then we would need to self-report on CIP-011-3 R1.5. If we have an employee with access to CIP Cyber Systems or Cyber Assets and not to BCSI and failed to remove the employee’s access then we would have to self-report on CIP-004-7 R5. If we have an employee that has access to both BES Cyber Systems and to BCSI and we fail to remove access in a timely manner then we have violations for both CIP-004-7 R5 and for CIP-011-3 R1. This isn’t an issue today because all access violations are rolled up to CIP-004-6 R5 but by separating them into two Standards we would be required to report on both and thus exposing us to multiple possible violations whereas today it would only be one.

Additionally, many Responsibly Entities’ Access Control procedures are written under CIP-004-6 - Access Control procedure. Everything an employee would need to know about their access control responsibilities would be located in a single document. This change would either create a potential compliance risk by breaking access controls up into separate documents or cause entities to perform significant changes to how they document their compliance procedures.

Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	
Comment	

Grouping by control type rather than CIP standard number is preferred. Access controls in many different areas of the standard does not add clearity.

Likes 0	

Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree with the transfer of all BCSI-related requirements from CIP-004 to CIP-011. Duke Energy concludes that moving access revocation requirements from CIP-004 to CIP-011 will create the potential for access revocation of an individual entity violating requirements in two separate standards.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
There are two separate ways of evaluating this question. On one hand, it seeks to create a common place to include requirements on information protection. On the other hand, it breaks the previous approach to consolidate all access authorization, provisioning, revocation, and deauthorization. By moving these requirements, it also potentially changes a single violation for CIP-004 R4 or R5 into multiple violations.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the shift of BCSI access authorization and revocation from CIP-004 to CIP-011. This allows an entity the option to have different processes in place for granting and removing access to BCSI if they desire and removes the implied requirement of having a Personnel Risk Assessment (PRA) executed before access to BCSI is granted if the entity does not what to make that a requirement in their environment.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike

Answer	Yes
Document Name	

Comment

However, the SDT should modify the applicability in CIP-011-3 requirements to align with CIP-004.

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	Yes
Document Name	

Comment

SNPD supports this change. CIP-004 should address BCS while CIP-011 should address BCSI (physical vs logical access). Mixing access and storage requirements across multiple CIP standards is confusing and increases the likelihood for mismanagement.

Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	Yes
Document Name	

Comment
Yes, however it is worth acknowledging that R3 applies to disposal/redeployment of cyber assets, not BCSI. Additionally, we suggest making separate requirements for BCSI on premises versus in the cloud. This way there can be no implication that something new is required for BCSI on premises, such as it appears currently with key management (R2).

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment
Yes it will make changes to CIP-011 easier in the future, but it also allows for ease of changes in the future which makes it easier to include Low Impact. This was brought up on the webinar that the scope of the SAR does not include Low Impact, but this change will easily allow changes to the standard to include Low Impact without unintended consequences to other standards/requirements.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3	
Answer	Yes
Document Name	

Comment
AEP agrees these changes have the potential to provide greater clarity surrounding BSCI and BCS. However, please see AEP’s comments to questions #8 and #9.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Black Hills agrees that placing all the BCSI requirements into one standard provides clarity. However, we think it would be beneficial to modify the language taken from CIP-004, making it less rigid.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Overall yes; however, some third party issues remain to be addressed. See NPCC RSC comments.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Yes, however it is worth acknowledging that R3 applies to disposal/redeployment of cyber assets, not BCSI. Additionally, Tri-State suggests making separate requirements for BCSI on premises versus in the cloud. This way there can be no implication that something new is required for BCSI on premises, such as it appears currently with key management (R2).	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes

Document Name	
Comment	
Moving the BCSI requirements from CIP-004 to CIP-011 as proposed is OK with MEAG. It doesn't matter if the BCSI requirements are all in 1 standard or multiple standards.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Comments: Yes it will make changes to CIP-011 easier in the future, but it also allows for ease of changes in the future which makes it easier to include Low Impact. This was brought up on the webinar that the scope of the SAR does not include Low Impact, but this change will easily allow changes to the standard to include Low Impact without unintended consequences to other standards/requirements.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
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	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	

11. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

William Hutchison - Southern Illinois Power Cooperative - 1

Answer	No
Document Name	

Comment

Comments: Yes, an Entity without ERC today will now be required to have an information protection program which could have a major impact. What is the risk sought to be reduced here? There is not a possibility to use a site without ERC as a pivot point, so the likelihood of a site without ERC being used in a cyber-attack is incredibly low. Increasing the scope here only furthers the point from question 10 on easily increasing scope in the future.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

This will add workload that may may not be justified by risk. Devices without ERC have less IT security risk than routable devices.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1, R4.4, R5.3 when moved them to CIP-011-3 R1.3, R1.4, and R1.5 is unacceptable. This “with ERC”deletion expands the scope of CIP-004 R4 and R5 requirements signicantly. After this scope expansion, CIP-004 R4 and R5 requirements will not only apply to all locations of BCSI pertaining to Medium Impact BES Cyber Systems, but also apply to all Medium Impact BCS since the Medium Impact BCS contains BCSI. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself and this is why the current CIP-004 R4 and R5 don’t apply to Medium Impact BCS without ERC.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is concerned about the expansion of scope introduced by these changes. Are they warranted from a security standpoint, given that BSCI about a Medium substation without ERC, for example, likely presents less risk to the BES than the network information about a Low substation with ERC (which is not even covered at all). Considerable additional resources will need to be expended to protect BCSI that may not present a significant security risk, apparently only for the reason of consistency in wording. See also response to Question 2, above.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

It would be helpful if SDT provide some rationale for expanding the applicability to PCA. This expansion is not reflected in the Standard Authorization Request. We need to ensure that additional compliance burden pays off in mitigating the security risk.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	
AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	
Comment	

Yes. NRECA believes the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. The SAR explicitly stated that the purpose or goal of the project was "[c]larifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information." Further, the scope of the SAR did not make any mention of scope expansion. In fact, the SAR explicitly provided for modifications to "clarify" existing access management requirements for BCSI. Accordingly, because the SAR did not contemplate or authorize scope expansion relative to asset applicability, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, ***the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s)***. The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, *CIP-011-2 should also be evaluated for any* ***subsequent*** *impacts*.

Further, NRECA notes that PCAs currently do not require authorization for access in CIP-004. If no access authorization is required to access the asset itself, it is unclear as to why authorization would be required to obtain access to information about a system for which no access authorization is required. This contradiction is not addressed within the Technical Rationale and should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to add PCAs to CIP-011.

Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment	
Agree with MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Yes. First, GSOC respectfully suggests that the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that the purpose or goal of the project was "[c]larifying the CIP requirements and measures related to both managing access and securing BES Cyber System Information." Further, the scope of the SAR did not make any mention of scope expansion. In fact, the SAR explicitly provided for modifications to "clarify" existing access management requirements for BCSI. Accordingly, because the SAR did not contemplate or authorize scope expansion relative to asset applicability, the SDT revisions go beyond the scope of the SAR as provided below (emphasis added):

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, ***the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s)***. The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g. cloud services). The current Requirements are focused on access to the "storage location", but should consider management of access to BCSI while in transit, storage, and in use. In addition to CIP-004-6 modifications, *CIP-011-2 should also be evaluated for any* ***subsequent*** *impacts*.

Further, GSOC notes that PCAs currently do not require authorization for access in CIP-004. If no access authorization is required to access the asset itself, it is unclear as to why authorization would be required to obtain access to information about a system for which no access authorization is required. This contradiction is not addressed within the Technical Rationale and should be addressed by the SDT to ensure that there is an appropriate identification of risk associated with the recommendation to add PCAs to CIP-011.

Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

SMEC agrees with comments submitted by NRECA.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Yes, an Entity without ERC today will now be required to have an information protection program which could have a major impact. What is the risk sought to be reduced here? There is not a possibility to use a site without ERC as a pivot point, so the likelihood of a site without ERC being used in a cyber-attack is incredibly low. Increasing the scope here only furthers the point from question 10 on easily increasing scope in the future.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

This seems to defeat the SDT's stated intention to focus the security on the BCSI; therefore, in its proposed form the requirement language neither aligns with nor accomplishes this stated objective

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

See NRECA submitted comments.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST does not have any concerns with the proposed expansion of CIP-011 to include PCAs. N&ST notes that the current, enforceable CIP-011-2 is already applicable to all Medium Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	No
Document Name	

Comment

Oncor does not agree with the scope expansion unless the SDT provide justification that pay off additional burden in mitigating the security risk.

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf. Additionally, SDG&E would like to comment on CIP-011-3 requirement's proposed inclusion of all Medium-Impact BCS, regardless of ERC. The current CIP-004-6 R4.4 requirement specifies applicability for only High Impact BCS and Medium Impact BCS with ERC. The new CIP 011-3 brings all BCSI in scope regardless of ERC in Medium-Impact Sites. This change is significant and overburdensome to sites that don't currently fall into this category of BCSI.	
Likes 0	
Dislikes 0	
Response	
Ayman Samaan - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

We are concerned because of access management associated with Medium Impact.

This expansion is not backwards compatible

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No – PCA may also contain BCSI.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

PCA may also contain BCSI.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

We may in the future.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
We may in the future.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6, when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E has concerns regarding the addition of PCA and the benefit of including them compared to the effort of identifying and protecting BCSI related to PCA. As noted in Question 5, PG&E would like the SDT to articulate the reason for the addition of PCA since there is no information in the Technical Rationale document to warrant its addition.

Regarding the inclusion of all Medium Impact BCS, PG&E believes this is an appropriate modification since the BCSI information for these Cyber Assets could be used to compromise those Cyber Assets if physical access is gained.

Likes 0	
Dislikes 0	

Response

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower supports Duke Energy's comments. This creates a possibility of multiple violations as opposed to a single violation in the original CIP-004 Standard.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
We are concerned with scope creep. What problem are we trying to solve?	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy is concerned that increasing the Applicability of the Requirements to include the addition of PCAs and all Medium Impact BCS would require significant efforts to modify technical, administrative, and operational controls, compliance processes, and evidentiary documentation. Duke Energy suggests to consider surveying Responsible Entities to assess how many PCAs and Medium Impact BCS would now need to comply with CIP-011-3 and at what cost vs. the potential increase in Reliability to the BES.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
More clarity is needed.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3, is unacceptable. This deletion greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself.

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as any such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. These Cyber Systems can only be compromised by breaching physical security, in which case this standard provides no protection.

Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

The addition of PCAs is overburdensome. By definition, PCAs do not have a 15 minute impact on the reliability of the BES. They are not a part of a BCS and should not be considered BCSI.

Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy support the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	Yes
Document Name	
Comment	
Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State does not agree with the scope expansion, as the risk associated with these added assets is much lower. This does not conform to the risk-based approach that the ERO has been striving to. The SDT would need to provide justification for scope expansion, especially given this was not in scope of the SAR.	
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	

Suggest retaining existing scope that includes exclusions for Medium without ERC. The security posture of a system without ERC substantively decreases the value of BCSI for remote attack scenarios, thus greatly reducing the value of that information to a potential adversary.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment

AEP agrees with EEI, and does not support the addition of PCAs and Medium Impact Assets without ERC because the SDT has not adequately described the risks or provided an explanation that justifies the expanded compliance burdens for entities. These changes go beyond the scope of the SAR and improperly expands the scope of protections beyond the currently approved CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We are concerned because of additional effort that imposing access management associated with BCSI for Medium Impact BCS (without ERC) and PCAs
While IESO has only High Impact BCS, further analysis would need to be done to determine the amount of the impact on Ontario market participants where this applicability would apply

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

The proposed changes will add a considerable amount of work to any utilities that have Medium Impact Assets without ERC which may not be justified by risk. Devices without ERC have less IT security risk than routable devices.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	

Comment

AZPS is concerned that the proposed expansion of CIP-011-3 to include Protected Cyber Assets and all Medium Impact Assets is unnecessary and may be overly burdensome on Responsible Entities. AZPS believes the protections already afforded to these assets through the implementation of CIP-005-5 and CIP-006-6 are sufficient to protect against any unauthorized “use” of BCSI.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3

Answer	Yes
Document Name	

Comment

Tri-State G&T does not agree with the scope expansion, as the risk associated with these added assets is much lower. This does not conform to the risk-based approach that the ERO has been striving to. The SDT would need to provide justification for scope expansion, especially given this was not in scope of the SAR.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment
Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself. The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI. Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
As always, the cyber risk is not well-addressed by rating cyber systems by association with physical BES assets and facilities. The risk from cyber attack is the speed of exploit. Automation and vulnerabilities on one machine can be exploited and spread exponentially through networks infecting all other assets within a similar security profile or to which an unprotected or poorly secured connection exists. So the cyber risk and the impact to the particular BES asset to which it is attached are not a good proxy for each other. The risk to the BES of lots of poorly secured cyber assets is that in concert they can have a disparately large impact to multiple BES assets. Aggregate attacks on low impact cyber assets can equate to a moderate level of impact, and likewise attacks on (individually) medium impact assets can have a high impact when aggregated across a large number of such facilities.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment

Dominion Energy supports the work the SDT has done on develoing the current draft. Dominion energy suggests that the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue and further supports EEIs comments. The potential expansion of the scope to these assets appears to be poutside the scope of the original SAR.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI 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

This scope expansion was **not** in the SAR and the Technical Rationale states it was added, but gives no rationale as to why it was added. What risk is being mitigated that justifies an increase in effort and cost? A case can be made that PCAs are already covered in the existing language since network diagrams and lists of all network clients are already included in the definition of BCSI. We suggest the SDT include a rationale for the addition in the Technical Rationale document and appropriately outline the risk that is being addressed.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes

Document Name	
Comment	
ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
We are concerned because of access management associated with Medium Impact would bring into scope a large number of information related to medium impact substations .	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Removing the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 R4.1 when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable and sufficient protection in and of itself. *The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.* *Having a lack of ERC also renders BCSI pertaining to Medium Impact BES Cyber Systems outside the scope of R1 Part 1.2, as such information, if obtained, cannot be used remotely, as there is no remote access to the Cyber Systems. Information pertaining to these Cyber Systems can only be used to compromise them by breaching physical security, in which case the CIP-011 standard provides no protection.*	

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

As described in the SAR, the changes were to add the ability to allow entities to use cloud services and to clarify the requirements and measures related to access and securing BCSI. We are unsure why the changes included expanding the scope to all Medium Impact BCS and PCAs. If approved as written, 18 months will not be sufficient time to implement this across this large number of new assets, locations and information. Additionally, an asset that has no impact on the BES and just resides within the same ESP as a BCS, a PCA, does not (by default) have BCSI.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	Yes
Document Name	

Comment

Please provide more clarity on the phrase "System information pertaining to". This needs to be well defined and understood. There may be many systems that are associated with systems that may or may not house BCSI.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	Yes
Document Name	

Comment

As a note, CIP-011-2 already applied to all Medium Impact whether or not External Routable Connectivity existed.

Adding PCA is a concern because it could be a major new effort unsupported by existing resources with expertise in OT, not IT, assets. Existing storage locations, especially for substation BCS, PACS, and EACMS may be using a file-based version control system that may only be configured and capable of handling a small number of text or firmware files. This system may not not be amenable to storing more complex configurations of a local PCA such as a terminal or server running Windows.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI cannot support the addition of PCAs and Medium Impact Assets without ERC because there has not been an adequate identification of the risks or an explanation for the expanded scope. These changes go beyond the scope of the SAR and expands the scope of protections beyond the currently approved CIP Reliability Standards. The SDT should limit the applicability of BCSI to what is currently approved in CIP-011-2. If the SDT is aware of any reliability gaps, it should develop a white paper to support their concerns and develop a revised SAR for approval.

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 NextEra

Answer	Yes
Document Name	

Comment

1. We are concerned because of access management associated with Medium Impact.

1. This expansion is not backwards compatible.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
1. BC Hydro considers that additional guidance on the interpretation of what constitutes BCSI within either the Standard or the definition of BCSI is needed for a more consistent framework across the industry. 2. With the expansion of scope to PCAs, BC Hydro requests that the language of the Standard includes provisions that limit the scope of authorization requirements only to information disseminated after the effective date of the standard, and clarity that audits of previously released information is not required.	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
SNPD does not understand what the new language is trying to achieve. We believe we understand and would likely choose to agree with the proposed change, but the language does not appear to provide the necessary descriptive clarity to differentiate between whether the standard is attempting to govern ALL PCA within medium facilities or just PCA with external connectivity? If the intent is ALL, please state so clearly.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI’s comments.	
Likes 0	
Dislikes 0	

Response
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3
Answer	Yes
Document Name	
Comment
See Steven Toosevich's comments.
Likes 0	
Dislikes 0	
Response
Constantin Chitescu - Ontario Power Generation Inc. - 5
Answer	Yes
Document Name	
Comment
OPG is in agreement with RSC provided comment
Likes 0	
Dislikes 0	
Response
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2
Answer	Yes
Document Name	
Comment
PGE agrees with EEI’s comments
Likes 0	
Dislikes 0	
Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
While the identification of BCSI has not increased in scope, the identification of BCSI storage locations has. This will add burden to entities that have many Medium Impact systems with no ERC. Additionally, the R1 Part 1.2 requirement language as written seems to make even authorized access impossible.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Removing the qualifying language “with ERC” from the applicability of Medium Impact BES Cyber Systems from CIP-004-6, when moved to CIP-011-3 R1.3, greatly expands the scope of this requirement. This expansion of scope is not justified, as the deliberate choice of not implementing ERC to Medium Impact BES Cyber Systems is currently recognized as a considerable protection.	

The scope is also expanded significantly by changing the former CIP-004 requirements to apply to all BCSI, not just designated storage locations of BCSI.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

There are several expansions of scope built into this proposed revision. CIP-004-6 Part 4.4 is applicable to only Medium Impact BES Cyber Systems with ERC. The ERC qualifier is removed as part of CIP-011-3 Part 1.3. While most Responsible Entities likely take care to protect BCSI to one degree or another, there is not a compliance threshold for authorizing access to BCSI associated with Medium Impact BES Cyber System without ERC. This proposed change increases the burden on Responsible Entities. Additionally, PCAs are introduced as associated devices in this proposed revision. Again, most Responsible Entities are likely protecting much of the information, and this creates a new compliance threshold and new compliance burden that Responsible Entities will have to bear. A signicant effort will be required to evaluate processes and procedures, to re-evaluate devices, provide training, update and change technologies that are used to authorize and approve access. There are concerns that this will take more than minimal effort to accommodate these changes without commensurate security benefits.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
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	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

12. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes the cost of meeting the Standard will be greater by instituting key controls and other prescribed processes that are unnecessary. It increases workload greatly.	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
The key management section needs to be better defined to show a difference between on premise and third party storage of BCSI. Solutions to the key management issue may prove costly depending on the scope of where it will need to be used.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. We believe the standard revisions will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.	

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E indicates the move of access authorization and revocation from CIP-004 to CIP-011 and inclusion of key management are appropriate in addressing the protection of BCSI. There could be increased costs related to key management if an entity does not have that current capability for key management but does not believe there would be any cost increase if an entity currently has a key management program.

For the addition of PCA, PG&E has concerns related to the benefit of their inclusion compared to the administrative burden of identifying and protecting that BCSI. As noted in Question 5, PG&E would like the SDT to articulate the reason for the addition of PCA to help determine if it should be covered by the Standard.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Light Company believe there is a more cost-effective approach as set forth in EEI's comments.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No

Document Name	
Comment	
As noted elsewhere, ERCOT believes some of the proposed changes may be administratively burdensome and that more cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive controls and focus more on objective or outcome based changes. ERCOT also notes that it is difficult to determine cost-effectiveness absent a complete draft standard.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. We believe the standard revisions will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
If it where cost effective it would NOT be so prescriptive. Please include the real cost in the estimates maybe $350K/year+? Remember the WECC Poka-Yoke webinar. Thorough project controls analysis; whatever can fail plan, will fail; so plan for cost of finding failures and fixing failures, then doing it again until no failures, include all this work WECC discusses in their webinar in cost estimates.	
Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
As noted above, some of the proposed changes are administratively burdensome and a more cost-effective solution may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive controls and instead be more focused on objective or outcome based changes. Additionally, it is difficult to determine cost effectiveness with the first draft of a standard.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
An evaluation would be needed to determine, but this proposal would likely add costs and does not appear to be cost effective as written. This recommendation will require additional time, attention, and coordination between several departments and subject matter experts.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with NSRF’s comments.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
No, the proposed changes do not meet the goal of enabling (relatively) easy vetting and procurement of cloud services or efficient use of cloud services without the need for onerous local key management, and will likely not result in adoption of cloud services for BCSI due to the increased resources required to vet, secure, and maintain BCSI in the cloud. Reciprocal federal certifications, such as those described in the response to Question 3, would greatly alleviate the resources required for small and medium sized Entities.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
If it where cost effective it would NOT be so prescriptive. Please include the real cost in the estimates maybe $350K/year+? Remember the WECC PokaYoka webinar. Though project controls analysis. Whatever can fail plan for those high costs in esimate too?	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro estimates that significant costs will likely be incurred, particularly in relation to R2 of CIP-011-3. Also the use of vendors will lead to significant costs relating to risk assessments under R1.4. If vendors need to adhere to entity imposed Vendor controls, the costs may be passed back to the responsible entity. More cost effective approach would be to establish an industry accceptable standard for vendors and, if they meet these criteria, this would negate vendor risk assessments as part of reliability standard requirements. This could be done by creating a list of certified vendors for entity use.	

Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

As noted in our response to questions 6 and 8 above, some of the proposed changes are administratively burdensome where more efficient and cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs; it would seem that a less prescriptive method favoring an objective / outcome-based requirement would be a better approach. Cryptosystems and key management may be cost prohibitive for many organizations.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Unintentionally, check a response to question 12. EEI offers no response to question 12.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

No. As noted in our response to questions 6 and 8 above, some of the proposed changes are administratively burdensome where more cost-effective solutions may be available. Recognizing that complying with new regulations will lead to increased costs, a more cost-effective approach may be to focus on less prescriptive methods in favor of objective / outcome-based requirements.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support MRO comments.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We believe that the proposed changes, which include the changes for cloud-based solutions and the increased scope for Medium Impact and PCAs, are not a cost-effective approach.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The changes included will require additional cost to every entity in North America, primarily through increased staff needed for compliance management. Also, the additional cost associated with the change to Medium Impact expanded scope.

Likes 0	
Dislikes 0	

Response

Ayman Samaan - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please see comments submitted by Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security.

We belive the standard revisons will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response found in the NSRF Comment Form	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf. SDG&E believes the new requirements will increase costs for the Responsible Entities.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
See response to question #11.	
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 agrees with other industry organizations, particularly NSRF, where the proposed changes will significantly increase the compliance and documentation burden without a commensurate increase in security.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	No
Document Name	
Comment	
NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy does not have enough information to make an informed cost effectiveness conclusion.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

This is very difficult to quantify across all of industry and various types of registered entities. If the language can be adjusted to account for non-electronic information storage locations, it has potential.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security.

We belive the standard revisons will increase the risk of non-compliance due to some of the proposed requirements having impossible evidencing requirements.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes the costs associated with moving CIP-004 access management requirements to CIP-011, with changing the objects of access management from BCSI storage locations to BCSI, with being required to perform annual risk assessments of 3rd-party BCSI storage vendors, and with implementing prescriptive key management program requirements could be significant. At the same time, N&ST believes these proposed changes would neither achieve the SDT’s stated goals nor improve the security of BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	No
Document Name	
Comment	
Tri-State expects the proposed changes, as drafted, to be costly. For example, Part 2.2 prescribes a segregation, without any consideration of controls, that could 1) prevent an entity from utilizing a cloud solution and instead having to pay the more expensive rate for on premise solution, 2) prevent an entity from being able to fully implement into a cloud solution (which means managing and paying for both cloud and on premise environments), or 3) result in a substantial increase in costs associated with managing keys on premise with additional staff, or by a 3rd party.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Given the duplicity of these proposed modifications with other current or future enforceable standards, these revisions are too prescriptive and introduce undue administrative burden without accomplishing the SDT’s stated objectives. In addition, moving CIP-004 requirements into CIP-011 has unintended consequences and does not achieve the perceived efficiency.	
Likes 0	
Dislikes 0	
Response	

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
AZPS is unable to make a determination of cost effectiveness at this time due to uncertainties in the requirements as currently drafted.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The proposed changes are not a cost-effective approach for a utility that does not ERC. These organizations will now have to look at their Medium Impact Asset documentation and decide what will become BCSI and then create storage locations for the information.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The potential costs of the Part R1.4 vendor controls may not produce an effective result. In addition, the submitted feedback to Standards Efficiency Review tends to question the value of annual reviews for the sake of a review. We would prefer a specific trigger or sets of triggers for reviews.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	No
Document Name	
Comment	
Because of the increases in scope of the standard this could have significant cost increases for REs making using 3rd party storage solutions cost ineffective.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The proposed changes increase compliance activities and burden without the likelihood of an associated increase in reliability or security. Further, several of the proposed changes would result in infeasible and impracticable compliance obligations. For example, as discussion above in GSOC's response to question #, the proposed revisions regarding the identification of BCSI would require a demonstration that all system information has been evaluated for classification as BCSI. Such is infeasible. Another example is the revocation requirements set forth in requirement R1.5, which, when coupled with the new requirements around identification of BCSI, would require that Responsible Entities prove that they successfully revoked access to every, possible, individual piece of BCSI. Such is not feasible and is a paper exercise that is not cost-effective or beneficial to reliability or security. Further, ambiguity around the term "sanitization" raises concerns that it unnecessarily raises the bar and reduce flexibility regarding what needs to be done to an asset prior to reuse of disposal. This creates uncertainty and increases the burden of compliance on Responsible Entities for no ostensible enhancement to reliability or security. This proposed revision and its consequences further impact overall cost-effectiveness of the proposed revisions as entities that cannot segregate storage media from the overall asset will either have to sanitize the entire device or destroy the entire device, neither of which results in a cost-effective solution for entities. Taken together, the proposed revisions do not propose substantive enhancements to security or reliability that would justify the additional cost, resource, or compliance burden or risk.	

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

Agree with MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

Based on our comments above, the proposed revisions do not propose substantive enhancements to security or reliability that would justify additional costs/resources.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments filed by NRECA

Likes 0	
Dislikes 0	

Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	
Comment	
AEP does not feel as though these changes are a cost effective approach. These changes will require additional training for employees due to requirements shifting to a different standard. Additionally, managing cloud service encryption and keys can be potentially expensive. However, AEP recognizes that cost-related circumstances vary by Responsible Entity.	
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	
This has the effect of ever increasing scope to include anywhere an instance of BCSI may reside, whether in a physical and/or logical form. If an individual were to create a paper copy of a BCSI, the entity would be obligated to track that paper until its destruction to ensure that it managed access to the BCSI. The additional review, controls, risk assessment, and significant expansion of the scope of this compliance obligation as written would have a high cost for the entity.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State expects the proposed changes, as drafted, to be costly. For example, Part 2.2 prescribes a segregation, without any consideration of controls, that could 1) prevent an entity from utilizing a cloud solution and instead having to pay the more expensive rate for on premise solution, 2) prevent an	

entity from being able to fully implement into a cloud solution (which means managing and paying for both cloud and on premise environments), or 3) result in a substantial increase in costs associated with managing keys on premise with additional staff, or by a 3rd party.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Seattle is unconvinced that the proposed changes represent a cost-effective approach, given the complexity of the required approaches; the unresolved questions about “obtain and use,” storage locations, R2 conflict with CIP-013, etc; and the prescriptive nature of new requirements R1.4, R1.5, and R2 that once again presume certain (although different) technology concepts that will no doubt soon become obsolete.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. The requirements are beyond the goals of SAR. The goals of SAR are to clarify the CIP requirements and measures related to both managing access and securing BES Cyber System Information and clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Likes 0	
Dislikes 0	

Response

Jeremy Voll - Basin Electric Power Cooperative - 3

Answer	No
Document Name	

Comment

Support the MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Refer to question 11.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The proposed changes significantly increase the compliance and documentation burden without a commensurate increase in security. The requirements are going well above and beyond the SAR, and as written requires more controls than are necessary to mitigate risks. For example, peforming vendor risk assessments at least once every 15 calendar months may not be commensurate with the low level of risk a vendor may pose, or there are no changes in the vendors practices that would warrant another assessment.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	No

Document Name	
Comment	
The standards may not reach the goal of allowing industry to leverage the lower cost of cloud services.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
R2.1 is not cost effective as written as it implies all BCSI must be encrypted.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
NOT COST EFFECTIVE. There is too much approach-uncertainty and therefore difficult to specifically identify safetly and risk mitigation methods. the proposed updates are adding administrative paperwork which does not improve BES security.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No

Document Name	
Comment	
The proposed recommendations will provide additional options for protecting BCSI as well as open to more technologies. Additionally, the proposed changes increase the required controls which will reduce risk and increase security. However, these changes are not cost effective and will require investment from entities to implement due to the increased controls and need to protect BCSI throughout the entire lifecycle as well as the increased need to protect BCSI stored in BCS, EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy thinks that the proposed recommendations from the SDT would require significant efforts to modify technical, administrative, and operational controls, compliance processes, and evidentiary documentation which carry a high cost and may be ineffective or outdated by the time of implementation.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Comments: Because of the increases in scope of the standard this could have significant cost increases for REs making using 3rd party storage solutions cost ineffective.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	

Answer	No
Document Name	
Comment	
Not for small entities.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Any changes to Standards with additional obligations does create costs.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Angela Gaines - Portland General Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
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 NextEra	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	

Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
Depends on clarifiaction to question 11.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
This cannot be answered until a more thoughtful consideration is given to third-party security objectives.	
Likes 0	
Dislikes 0	
Response	

13. Do you have any other general recommendations/considerations for the drafting team?	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

We feel by including all Medium Impact BES Cyber Systems and eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity, this draft of the standard exceeds the scope of the FERC-approved SAR, and does so to no gain while adding significant burden.

The aims of the SAR can be better and more easily achieved by:

1. Defining BCSI Repository

2. Defining BCSI Access

3. Focusing on managing BCSI Access to BCSI Repositories

Likes 0	
Dislikes 0	
Response	

Jeremy Voll - Basin Electric Power Cooperative - 3	
Answer	No
Document Name	
Comment	

Support the MRO NSRF comments

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	

AECI supports comments filed by NRECA	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with comments submitted by NRECA.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In general, PacifiCorp supports EEI and NSRF’s comments proposed for these revisions.	

By eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the FERC SAR.

Many of the proposed changes are not in scope with the SAR and are too prescriptive.

Removing CIP-004 R4.1.3, R4.4, & R5.3 – creates a perceived gap within the access controls designed for CIP-004. We suggest the removal of, “access to BES Cyber System Information (BCSI)”and the replacement with the term “BCSI Respository” or “designated BCSI storage location.” Thusly, termination actions would result in the removal of access to BCSI Repositiories.

If access controls are to be spread throughout the CIP suite of Standards then the references need to be made in both requirements to direct the readers to the correct locations.

CIP-011 R1.1 (A) – Applicable Systems not applicability. Suggested requirement language: Method(s) to identify information that meets the definition of BES Cyber System Information.

CIP-011 R1.1 (B) – Applicable Systems – change to Medium Impact with ERC. Suggested requirement language: Method(s) to identify designated BES Cyber System Information storage locations.

CIP-011 R1.2 - Applicable Systems not applicability. Suggested requiremenet language: Procedure(s) to prevent unauthorized access to BES Cyber System Information during storage, transit, use, and disposal.

CIP-011 R1.3 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Process(es) to authorize access to designated BES Cyber System Information storage locations based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.

CIP-011 R1.4 – Remove this requirement and add to CIP-013 where most appropriate.

CIP-011 R1.5 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: For termination actions, revoke the individual’s current access to designated BES Cyber System Information storage locations, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.

CIP-011 R1.6 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Verify at least once every 15 calendar months that access to designated BES Cyber System Information storage locations, whether physical or electronic, is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.

CIP-011 R2 – Suggested language: Each Responsible Entity shall implement one or more documented cryptographic key management program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Cryptographic Key Management Program.

The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive, with the list of things that should be included. The stated purpose of the SAR is referring to “cryptosystem” key management, but the NERC webinar slide regarding this part listed “physically.”

CIP-011 R2.1 – change Applicability to include “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories”. Suggested requirement language: Where applicable, develop a cryptographic key management process(es) to restrict access with revocation ability, shall include the following: (list of requirement sub parts)

CIP-011 R2.2 – change Applicability to include “BES Cyber System Information stored in Vendor managed electronic BCSI Repositories”. Suggested requirement language: Implement controls to separate the BES Cyber System Information custodial entity’s duties independently from the cryptographic key management program duties established in Part 2.1.

CIP-011 R3 – the requirement is fine as proposed.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	No
Document Name	

Comment

NCEMC supports the comments by Barry Lawson, National Rural Electric Cooperative Association and ACES

Likes 0	

Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	

Comment
SDG&E supports EEI's comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	

Comment
ITC supports the response found in the NSRF Comment Form

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
In general, we support EEI and MRO NSRF comments proposed for these revisions. *By eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the mandate of the SAR.*

Many of the proposed changes are not in scope with the SAR and are too prescriptive.

Removing CIP-004 R4.1.3, R4.4, & R5.3 – creates a perceived gap within the access controls designed for CIP-004. We suggest the removal of, "access to BES Cyber System Information (BCSI)"and the replacement with the term "BCSI Respository" or "designated BCSI storage location." Thusly, termination actions would result in the removal of access to BCSI Repositiories.

If access controls are to be spread throughout the CIP suite of Standards then the references need to be made in both requirements to direct the readers to the correct locations.

CIP-011 R1.1 (A) – Applicable Systems not applicability. Suggested requirement language: Method(s) to identify information that meets the definition of BES Cyber System Information.

CIP-011 R1.1 (B) – Applicable Systems – change to Medium Impact with ERC. Suggested requirement language: "Method(s) to identify designated BES Cyber System Information storage locations [or Repositories]."

CIP-011 R1.2 - Applicable Systems not applicability. Suggested requiremenet language: Procedure(s) to prevent unauthorized BCSI Access during storage, transit, and use.

CIP-011 R1.3 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Process(es) to authorize access to designated BES Cyber System Information storage locations based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.

CIP-011 R1.4 – Remove this requirement and add to CIP-013 where most appropriate.

CIP-011 R1.5 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: For termination actions, revoke the individual's current access to designated BES Cyber System Information storage locations, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.

CIP-011 R1.6 – Applicable Systems – change to Medium Impact with ERC. Suggested requiremenet language: Verify at least once every 15 calendar months that access to designated BES Cyber System Information storage locations, whether physical or electronic, is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.

CIP-011 R2 – Suggested language: Each Responsible Entity shall implement one or more documented cryptographic key management program(s) that collectively include the applicable requirement parts in

CIP-011-3 Table R2 – Cryptographic Key Management Program.

The draft requirement R2.1 regarding key management is unclear, and yet, at the same time, too prescriptive, with the list of things that should be included. The stated purpose of the SAR is referring to "cryptosystem" key management, but the NERC webinar slide regarding this part listed "physically."

CIP-011 R2.1 – change Applicability to include "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories". Suggested requirement language: Where applicable, develop a cryptographic key management process(es) to restrict access with revocation ability, shall include the following: (list of requirement sub parts)

CIP-011 R2.2 – change Applicability to include "BES Cyber System Information stored in Vendor managed electronic BCSI Repositories". Suggested requirement language: Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the cryptographic key management program duties established in Part 2.1.

CIP-011 R3 – the requirement is fine as proposed.

Likes 0	
Dislikes 0	

Response
Ayman Samaan - Edison International - Southern California Edison Company - 1
Answer	No
Document Name	
Comment
Please see comments submitted by Edison Electric Institute
Likes 0	
Dislikes 0	
Response
Wayne Guttormson - SaskPower - 1
Answer	No
Document Name	
Comment
Support MRO comments.
Likes 0	
Dislikes 0	
Response
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1
Answer	No
Document Name	
Comment
In general, we support EEI and MRO NSRF comments proposed for these revisions.
Likes 0	
Dislikes 0	
Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
In general, we support EEI and MRO NSRF comments proposed for these revisions.	
Likes 0	
Dislikes 0	
Response	
William Hutchison - Southern Illinois Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karl Blaszkowski - CMS Energy - Consumers Energy Company - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lynd - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwayne Parker - CMS Energy - Consumers Energy Company - 4	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colleen Campbell - AES - Indianapolis Power and Light Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
While the changes are a good start, significant consideration needs to be performed to consider the various environments the standard will apply to: (1) Information stored by the Entity, which includes many small Entities on both OT and IT systems; (2) Information stored by a Cloud service provider on behalf of an Entity; (3) Information located at a vendor under non-disclosure agreement in active use to meet BES needs.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Small agencies have limited budgets and staff. This approach continues to burden small agencies and we struggle to see any of the proposed changes being cost effective.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - SERC, Group Name Duke Energy	

Answer	Yes
Document Name	

Comment

Duke Energy recommends the following:

- Removing the periodic review requirement in Part 1.4, and allowing the risk assessment to determine necessary reviews and frequency;
- Need more clarity on where or when “factory resets” of a device are sufficient sanitization in reference to Part 3.1;
- R1.2 language is problematic

o Need clarity that we are addressing “unauthorized” ability to obtain

o Eliminate is extremely strong wording

o Likely would require extensive encryption implementation

o Addition of disposal is unclear – do they mean obtaining access after it’s been disposed? Prior to secure disposal;

o Consider the Glossary of Terms used in NERC Reliability Standards: “Operating Plan; Operating Procedure; and Operating Process, for use here and in Part 1.3 rather than “method”, or “process” For greater clarity as to SDT intent.

- R1.3 language is problematic

o How would we authorize access to information in use in a meeting, for example? Are we excpted to keep track of every vendor who has a short term / in-use need to know?

o It would be better to continue focusing authorization for access to storage locations and make that more robust; and

- R1.4 does this presume the Entity has authorized the vendor personnel to access the information (as is typically necessary to store it)? If not, the language is problematic.

o Additionally, do R1.5 and R1.6 apply to these vendor personnel?

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	Yes
Document Name	

Comment

Please increase outreach and collaboration using an approach to reach everyone. More than one meeting on specific topic may be needed to reach everyone due to other meeting conflicts and committments. Add written clarity to the Standards so it can stand on its own without needing supporting documents.

A guiodeline WILL be needed. Why not improve the Standard by increasing clarity thereby reducing the need for a Guideline?	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Please provide guidance on the requirements as they relate to encrypting BCSI stored by a Vendor and encrypting BCSI stored on premises.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
We recommend that the scope of the standards team consider leveraging standards such as Fedramp to justify the use of cloud services. We also recommend that the team revist the definition of BES CSI to clear ambiguity. The language and scope of the SAR focused on the resolution of the issue related to the physical control of BES CSI information in transit or use that may not be practical.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy support the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Comments:

-
  - CIP-011-3 R2 Part 2.1 introduces nine terms in its sub-parts 2.1.1 through 2.1.9. These nine terms are not further discussed or defined. While formal Glossary definitions may not be needed, each term should be at least briefly explained. For example, “2.1.1 Key generation – the methods used to create a new encryption key.” Of particular interest is the use of the term “Key suppression.” This term should be clearly explained.
-
  - The SDT should consider the advisability of keeping CIP-011-3’s BES Cyber Asset Reuse and Disposal as Requirement R2 for continuity with CIP-011-2.
-
  - Per CIP-011-3 R3 Part 3.1 that states “Prior to the release for reuse or disposal of applicable Cyber Assets (except for reuse within other systems identified in the “Applicable Systems” column), the Cyber Asset data storage media shall be sanitized or destroyed”, can the referenced Applicable Systems be reused by another entity without adhearing to CIP-011-3 R3 Part 3.1? For example; if parent company A decides to let company B reuse an Applicable System does the company A have to perform its CIP-011-3 R3 Part 3.1 process?
-
  - Is CIP-011-3 R1 Part 1.5 actually feasible for BCSI residing on externally controlled third party systems?

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	Yes
Document Name	2019-02_Unofficial_Comment_Form_201912_MH.docx

Comment

We would suggest making the following changes:

1. Define BCSI Repository (see our definition in Q1)

2. Delete CIP-011-3 R1.3 and R1.5 and make changes in CIP-004-6 (delete existing Part 4.1.3 and Part 4.4) as follows:

See the table provided in response to questions 13 in the attached comment form.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Seattle City Light appreciates the thorough efforts of the 2019-02 Standard Drafting Team to develop more flexible approaches to securing BCSI. We are keenly aware of the many difficulties and pitfalls associated with this endeavor.

Seattle believes, however, that an objective-based approach consistent with and similar to that employed in CIP-013 would provide a more effective solution and avoid the pitfalls and challenges. Specifically, revisions to CIP-004 and CIP-011 might better employ approaches based on a specific security objective (e.g., restrict access of unauthorized individuals to BCSI) and a risk-focused security plan rather than specific controls (control access to BCSI using keys managed by specific practices, etc), combined with requirements for implementation and periodic review. Such an approach achieves the desired security outcome with the double benefit of 1) not precluding use of new technologies outside the control paradigm in use when the Standard was written (as is the case with cloud storage in today's physically-focused Standards) and 2) allowing maximum flexibility to meet the myriad data management methods employed by the hundreds of subject entities across North America.

Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

- We believe the SDT went beyond the scope of the SAR. For example, adding a risk assessment similar to CIP-013 was not in scope.
- Suggest making separate requirements for BCSI on premises versus in the cloud.
- Overall it is good to see a futuristic direction with the requirements adapting to technology changes however, some of the changes are too prescriptive and therefore do not encompass current and future capabilities of all technology. Prefer to see goal and objective based requirements, not prescriptive.
- As it relates to Part 1.4, we think there should be a distinction between vendors that are hosting BCSI for the Responsible Entity's use, versus companies that the Responsible Entity provides BCSI to for a project. For example, if the Responsible Entity provides BCSI to a regional entity for an audit, the use and storage of that BCSI by the regional entity should not be in scope of this requirement. Instead, those scenarios should already be addressed by the entity's methods for securing and protecting BCSI.

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	

1) The requirements should be outcome focused and not prescriptive to specific technologies or techniques.

2) The changes to the standard do not provide any clarification regarding the definition of BCSI. This has led to consistency issues across regions regarding what information is considered BCSI. The lack of a clearly understood definition of what comprises BCSI limits the ability to evaluate the security value of the proposed access controls.

Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	

AEP is appreciative of the SDT's hard work of developing these proposed modifications. However, we feel that additional revisions are required as shown by our comments. AEP is of the opinion that while on-site storage might be burdensome to some Responsible Entities, BCSI storage on cloud platforms or within third party facilities should be entirely optional. We believe that cloud storage is not a mature enough technology at this time to be able to match the security that on-site storage can provide. AEP also wants to state that given the level of change proposed, we ask that Responsible Entities be provided with more time to ensure compliance by pushing the enforcement deadline to a later date.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	Yes
Document Name	

Comment

NRECA believes the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

NRECA recommends that NERC develop a process to gain industry consensus on proposed changes to CIP standards prior to the formation of a standards drafting team for modifications that are not directed by FERC. Multiple standards drafting teams have spent significant time attempting to make modifications to the standards for which there is no industry consensus that the modification is needed. This places the Standard Drafting Team in an untenable position and consumes a substantial amount of industry resources without benefitting reliability or security.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

Many of the proposed changes are not in scope with the SAR, are too prescriptive, and cause confusion rather than provide clarification. We don't believe the current standards, as written, preclude the use of cloud storage vendors and encryption technologies. In light of the fact that the CMEP

Guidance came out after the SAR, we wonder if changing the standards is needed. If needed, any further clarification can be done via additional guidance.

We disagree with the change in R1, Part 1.1 from “Method(s)” to identify information” to “Process(es) to identify information.” This would cause programs which use a method to identify information to be non-compliant. The last example of evidence is one such method--One can know that something is BCSI (identify it) just by the fact that it is in a specified location or repository. Technical Rationale for CIP-011-2, Requirement 1, paragraph 4 states: *“The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity’s program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of* ***methods that the entity may choose to utilize for the identification of BES Cyber System Information****.”* [emphasis added] Measure could be re-written as such: Documentation that information stored in a specified location is considered BCSI.

We disagree with having requirements for disposal in two different parts (R1 Part 1.2 and R3 Part 3.1) as this could result in double jeopardy during audits as auditors review disposal procedures for compliance with R1 and then again with R3. This change exceeds the SAR, and R3 takes the focus off protecting the information (BCSI), which has always been the intent of this part and CIP-011 as a whole. R3 also brings all Cyber Assets into scope, not just those that contain BCSI. We propose removing disposal from R1 Part 1.2 and reverting back to the CIP-011-2 version of R2 asset reuse and disposal as separate requirements.

We do not see how chain of custody is a measure of sanitization or destruction. In addition, this term was rejected by commenters and the SDT of a prior version of the standard.

The proposed High VSL is not appropriate or in line with other standards. As it reads, any instance of unauthorized access automatically results in a High VSL. A breach is always possible even with a sound plan and implementation. We propose removing the additional High VSL altogether, or looking to other standards which base VSL on included parts of the plan, or number of instances.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC respectfully suggests that the removal of requirements form CIP-004-6 to CIP-011-3 was not authorized by the SAR for this project. In particular, the SAR explicitly stated that CIP-004 be modified and that CIP-011 be evaluated for any downstream type impacts. It did not authorize the wholesale removal of requirements from CIP-004-6. Accordingly, the SDT revisions go beyond the scope of the SAR as provided below:

CIP-004-6 Requirements need to be modified so management of access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow various methods for controlling access to BES Cyber System Information, storage location(s). … In addition to CIP-004-6 modifications, CIP-011-2 should also be evaluated for any subsequent impacts.

GSOC recommends that NERC develop a process to gain industry consensus on proposed changes to CIP standards prior to the formation of a standards drafting team for modifications that are not directed by FERC. Multiple standards drafting teams have spent significant time attempting to make modifications to the standards for which there is no industry consensus that the modification is needed. This places the Standard Drafting Team in an untenable position and consumes a substantial amount of industry resources without benefitting reliability or security.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive
We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

We recommend the SDT consider development of a standard just for cloud services. This will eliminate confusion and ambuiguity for the current standards.

Likes 0	
Dislikes 0	

Response

Vivian Moser - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	

Comment
AZPS considers the proposed CIP-011-3 to exceed the scope of the SAR; however, recognizes the intent to increase the security posture for BCSI. For this reason, AZPS offers the following recommendations for the SDT's consideration: • Revise the proposed language to better delineate between protection of BCSI in use, transit, and disposal, and access to BCSI storage locations. • Revise the applicability language to clearly establish focus on BCSI. As provided in our response to Question No. 5, AZPS offers the following suggested wording: "System information pertaining to (but not including the BES Cyber System (BCS) which may contain BCSI):…" • Reconsider the addition of CIP-011-3 R2 as currently drafted. AZPS asserts that requiring a key management program is overly prescriptive (see further comments on this requirement included in the AZPS response to Question No. 8).

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment
Several of the proposed revisions are outside of the SAR, and this draft is too prescriptive and absolute in its language, and therefore not risk-based nor technology agnostic. Additionally, within this comment form, the SDT did not seek feedback on the proposed language in Part 3.1. This proposed language is a step backwards and posed undue administrative burden without a commensurate security or reliability benefit. The requirements should be focused on security and reliability value, and sanitization or destruction of data storage media not containing BCSI does not provide security nor reliability value. In fact, for entities that may have life cycle processes in place to reuse equipment in a less critical capacity after a refresh in the critical environment (perhaps test or dev, as one example) the requirement as written precludes an entity from reusing a non-BCSI device with a known and standardized OS configuration, patch level, etc. in a different capacity outside the environment without a full sanitization and rebuild. This is an inefficient use of Registered Entity's limited resources.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We believe the SDT went beyond the scope of the SAR. For example, adding a risk assessment similar to CIP-013 was not in scope. Suggest making separate requirements for BCSI on premises versus in the cloud. Overall it is good to see a futuristic direction with the requirements adapting to technology changes however, some of the changes are too prescriptive and therefore do not encompass current and future capabilities of all technology. Prefer to see goal and objective based requirements, not prescriptive. As it relates to Part 1.4, we think there should be a distinction between vendors that are hosting BCSI for the Responsible Entity's use, versus companies that the Responsible Entity provides BCSI to for a project. For example, if the Responsible Entity provides BCSI to a regional entity for an audit, the use and storage of that BCSI by the regional entity should not be in scope of this requirement. Instead, those scenarios should already be addressed by the entity's methods for securing and protecting BCSI.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	NRECA comments 2019-02_Unofficial_Comment_Form_201912 (1) 013120.docx
Comment	
See NRECA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	

In order to properly shift the approach of information protection to focus on the information and not the storage locations, the requirement for declaration of storage locations must be either removed or eased to focus on information residing with a vendor or third-party provider (e.g. cloud.) In addition, information residing within a BCS environment should be fully exempt from this requirement as the existing CIP-004, CIP-005, and CIP-006 protections will protect the information as long as it does not leave the BCS environment.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

(1) N&ST recommends retaining the existing language of CIP-011-2 Requirement R1, Part 1.2 (“Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.”) In addition to objecting to the proposed “obtain and use” language in a revised Part 1.2, N&ST notes that as written and if interpreted literally, the proposed requirement would compel a Responsible Entity to ensure that NOBODY could “obtain and use” BCSI.

(2) While N&ST opposes moving existing BCSI storage location access management requirements from CIP-004 to CIP-011, we support the SDT’s proposals to modify CIP-011’s “Applicability” column entries and to add an explicit requirement to identify BCSI storage locations. N&ST believes that if this is done, the “Applicability” of CIP-004 requirements that apply to BCSI storage locations (R4 Part 4.1.3, R4 Part 4.4, and R5 Part 5.3) should be changed to “Identified BCSI Storage Locations.” N&ST understands this change would likely compel moving R4 Part 4.1.3 to a revised R4 Part 4.2 and renumbering existing R4 Parts 4.2 – 4.4 to R4 Parts 4.3 – 4.5.

Likes 0	
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	Yes
Document Name	

Comment

The NYSRC is casting NEGATIVE vote because of these concerns:

• We have a concern regarding Requirement 1.4, which calls for risk identification, assessment, and mitigation for entities choosing to use a vendor to manage their BCSI. The risk identification and assessment portion of the requirement overlaps with CIP-013. We would like to know why the SDT is requiring mitigation for CIP-011 compliance when it is not required for CIP-013 compliance. Also, this Requirement calls for a re-assessment at

least once every 15 months. We believe that the value that this would add to cybersecurity programs may be outweighed by the cost of performing the reassessment (and subsequent mitigation).

• There is ambiguity vis-à-vis the data destruction requirement for High & Medium Impact BES Cyber Systems. Does this apply to virtualized BES Cyber Assets? What about BES Cyber Assets with read-only memory?

• Requirement 2.2 – separation of duties between BCSI custodian and key-management custodian – will be difficult to implement for entities that use physical keys, since in those instances it will most likely be the same individual(s) responsible for both sets of duties.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Dominion Energy supports EEIs comments.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren agrees with and supports EEI 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

CIP-011 R3 has increased in scope from BES Cyber Assets that may contain BCSI to the sanitization or destruction of ALL data storage media for ALL BES Cyber Assets. This language removes from the Responsible Entity the ability to determine *if* a BES Cyber Asset contains BCSI, and if so, take measures to prevent the unauthorized retrieval of said BCSI, and in turn requires the sanitization or destruction of ALL BES Cyber Assets. What purpose is served by sanitizing or destroying an asset that does not contain BCSI? There is no rationale for this change documented in the Technical Rationale document. We believe this requirement to now be problematic as there may be BES Cyber Assets that are firmware based and thus have "data storage media" for their firmware code but have no capability to store BCSI. They are now in scope of this requirement, however there is no need (and may have no ability) to wipe their firmware code. This requirement then forces the destruction of those devices that cannot be sanitized but that do not contain BCSI, and this is an undue burden placed upon entities with **no** security benefit.

We also find that CIP-011 R3 is the one requirement that was explicitly hardware based, and it retains its hardware basis even though Question 9 implies that enabling cloud solutions would require the move away from hardware basis. The suggested change also presents issues with today's on-premise virtualized environments where a virtual BES Cyber Asset with virtual storage, the virtual storage may be destroyed but that is not technically the "data storage media". The entity may not be able to map a logical, virtual storage unit to the actual "storage media" in the underlay on which the data resided, and it cannot wipe or destroy physical media without impacting other live BES Cyber Assets.

We suggest the requirement simply state:

"Prior to the release for reuse or disposal of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of the BES Cyber System Information."

There should be a clear delineation between Affiliate Restrictions requirements (the Standards of Conduct) for protecting information which may include BCSI and the R1 Requirement of "Process to identify information that meets the definition of BES Cyber System Information…"

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

We have concerns with the Measures in Part 3.1 on "chain of custody" as too prescriptive.

We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

The effort put forth by the SDT is appreciated. However, we encourage the SDT to review the approved SAR and focus on adding requirements that meet the objective of clarifying protections for cloud-based service providers, while keeping the burden on entities that do not use cloud-based providers to a minimum. Additionally, while adding clarity around managing access to BCSI and securing BCSI, the SDT should consider how the changes might impact or be similar to other requirements and attempt to avoid instances of added confusion or spaghetti requirements (access management and vendor risk management). As stated in other drafting teams, the industry is looking for risk-based requirements, and adding more specificity to requirements defeats this concept.

Furthermore, there were no questions specific to the implementation plan, but as proposed today, 18 months does not seem sufficient. As discussed above, adding Medium Impact and PCAs could take significant time to implement across a large number of new assets, locations and information. Additionally, the vendor risk assessment could cause entities to modify their vendor agreements, which in turn could increase costs to the entities.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	Yes
Document Name	

Comment

Yes – MISO commends the SDT for its efforts to consolidate like requirements and suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 and ISO 27001.

In addition, MISO recommends that each requirement be reviewed and restated as applicable to focus on results; i.e. the protection of BES Cyber Security Information : prevent unauthorized access to BCSI (performance-based), perform testing/simulations that demonstrate inability to access BCSI without authorization (risk-based) and document procedures to prevent unauthorized access to BCSI (competency-based). Monitor performance via periodic reporting of test/simulation results, actual security breaches/events, other?

Finally, MISO proposes the issue of electronic disposal be addressed. MISO suggests the SDT consider updating CIP-011-3, requirement R3 to provide objective based requirements related to disposal. As written, the standard would be administratively burdensome from an evidence perspective.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Although EEI recognizes and appreciates the work done by the SDT to enhance entity options as it relates to the use of cloud-based services for the storage of BCSI, many of the proposed changes are not in the scope of the approved SAR and are too rigid. The SAR seeks clarifying language that would allow entities to safely and securely store BCSI on third-party cloud-based services. Thus, the change could be made through minor modifications, such as developing new definitions (i.e., “BCSI Repository” and “Useable Access”) along with a few minor changes as suggested in our response to question 4 (above). In addition, adding vendor assessment requirements into CIP-011, while also moving requirements from CIP-004 to CIP-011, seem to conflict with one another. To the extent the SDT is concerned about potential reliability gaps meriting the proposed changes, a new SAR should be developed with technical justification. EEI also notes that the SDT did not ask about the appropriateness of the Implementation Plan. Given the level of change proposed, specifically related to vendor contracts, entities will need at least 24 months to achieve compliance with these new requirements.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Language in part 1.2 does not align with the language in part 1.5, requiring a method to eliminate ability to obtain and use BCSI in one and revoke individual’s access to BCSI in the other. This language mismatch will lead to confusion. Also, sub-requirement 2.1.2 is missing.	

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	Yes
Document Name	

Comment

NYISO commends the SDT for its efforts to consolidate like requirements and suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 and ISO 27001.

In addition, NYISO recommends that each requirement be reviewed and restated as applicable to focus more on results and security objectives; i.e. the protection of BES Cyber Security Information : prevent unauthorized access to BCSI (performance-based), perform testing/simulations that demonstrate inability to access BCSI without authorization (risk-based) and document procedures to prevent unauthorized access to BCSI (competency-based).

Further improvements of the draft should consider:

- Separate and keep access authorization and revocation centrally maintained as part of CIP-004. Adding a reference to the CIP-004 requirements from within CIP-011. The related CIP-004 requirements should also be reviewed and updated.

- Clarify that Responsible Entities should determine protective measures for BCSI based on risk and that solution measures other than encryption may be acceptable.

- Keep together those requirements related to BCSI stored in environments owned by third parties (and in a way, that is not redundant).

- Clarify that vendor risk assessment requirement can be accomplished via CIP-013 SCRM program

- Adding clarification on the term, “obtain.” Would like assurance that we have a consistent understanding of what is meant between “Obtain and Use” versus “Obtain or Use.”

- NYISO agrees that all risk assessments requirements should be housed within CIP-013 and would suggest further clarification as to what type of vendor needs to be risk assessed dependent on the type of cloud service is being procured and used (e.g. IaaS, Paas

- All access should be revoked within the specified period for any reason where an individual no longer requires it, not just termination.

- NYISO definitely sees the benefit in key management conceptually, but the language is too ambiguous and confusing therefore, we cannot endorse it.

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 NextEra

Answer	Yes

Document Name	
Comment	
1) We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive. 2) We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Could there be a standard in providing some form of industry threshold qualifications to vendors to reduce the responsibility and remove the onus of entities subject to reliability standards to perform Vendor risks assessments and establish controls to mitigate these risks. Current model puts all pressures on entities to conduct all work on BCSI risk. Possibility to look at NIST / FedRAMP standards. Also please consider in providing additional guidelines on what constitutes "BCSI".	
Likes 1	BC Hydro and Power Authority, 5, Hamilton Harding Helen
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Please review the proposed language with an eye toward increasing the use of narrow scope. Explicit, and affirmative language is necessary to eliminate ambiguity and inspire confidence in not running afoul of compliance should an entity choose to store BCSI in the cloud. There should be no confusion as to what is and what is not permitted. Please investigate establishing reciprocity for Federal IT certifications.	
Likes 1	Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees with NSRF and EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Consider encompassing access management within one holistic Standard. The departure and movement of access management requirements amongst several Standards seem to be a step backwards from security integration and collaboration between programs.	
Likes 0	
Dislikes 0	
Response	

James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

- Overall, it appears that this version of requirements, specifically R.1.4, is intended to address situations where a Responsible Entity contracts with another party for the storage and processing of BCSI. With that intention, measures on each requirement would benefit from adding specific ways to demonstrate compliance when using a third party.
- Requirement R1.4 does not include minimum security requirements the risk assessments of vendors need to include, such as security training, access controls, and termination actions. A minimum set of expectations should be defined.
- Any requirements allowing the use of third party provider should also include measures on the use of external audits performed by accredited auditors (e.g. SOC) in demonstrating compliance with the requirement. This would include all access management and data destruction requirements.
- Can the drafting team provide more detail on the distinction between “data” about BES Cyber Systems and “information” about BES Cyber Systems? Although the distinction is made in the definition, the distinction is not addressed in requirements or measures. Usability of the information is the key.
- Part 1.3 should be moved to CIP-004 with the proposed language.
- Part 1.5 should be moved to CIP-004 with the proposed language.
- Requirement Part 2.2 should note that separation of duties is only necessary when a vendor or other third-party is housing the information. This should not be required if the information is stored on-premises with the Responsible Entity.
- Requirement Part 3.1 is redundant to Part 1.2.
- As the drafting team is considering updating the standards, suggest the existing standards evolve to align with industry security standards, such as NIST 800-53 / ISO 27001, and be more objective and outcome based changes.
- In reviewing this, it appears that the definition of BCSI should be modified to remove the examples. The definition allows for a risk-based approach to identifying BCSI but the examples are being used as an authoritative list and not as a form guidance. The examples should be removed from the definition and guidance written through other means.
- There appears to be no actual requirement for security awareness training for individuals with access to BCSI. CIP-011-3, R1.1, lists “training materials that provide personal with sufficient knowledge to recognize BCSI” as an example, not a requirement, of acceptable evidence. CIP-004-7, R2.1.5 requires training content on “Handling of BES Cyber System Information and its storage”, but this is applicable only to individuals with access to High and Medium Impact BES Cyber Systems~. This needs to be clarified to prevent a difference in interpretation between the Responsible Entity and the Auditor. Is has been noted that there is no requirement to perform Personnel Risk Assessments on individuals with access to BCSI.

Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG is in agreement with RSC provided comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5, Group Name PGE Group 2	
Answer	Yes
Document Name	
Comment	
PGE agrees with EEI's general recommendations, particularly that the SDT could pursue minor modifications, such as new definitions, to achieve the SAR's objective.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Without splitting EACMS into EACS and EAMS the issue of third-party analysis systems is not addressed but is included in the SAR. Please ensure that EACMS is split into EACS and EAMS in order to address this issue. Third-party analysis systems currently are include in the EACMS definition, splitting the definition would allow EAMS to be applicable within only the CIP-011 standard, and simplify use of these third-party services.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

We have concerns with the Measures in Part 3.1 on “chain of custody” as too prescriptive. We have concerns with Part 3.1 on demonstrating compliance with a) destruction of virtualized equipment and b) re-deployment of virtualized assets.

Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

ERCOT offers the following additional comments:

- Overall, it appears that this version of the requirements, specifically Part 1.4, is intended to address situations where a Responsible Entity contracts with another party for the storage and processing of BCSI. ERCOT believes there is benefit to including measures on each requirement that identify specific ways to demonstrate compliance when using a third party.
- Part 1.4 does not include minimum security requirements the risk assessments of vendors need to include, such as security training, access controls, and termination actions. ERCOT believes a minimum set of expectations should be defined.
- ERCOT believes that any requirements allowing the use of third party providers should also include measures on the use of external audits performed by accredited auditors (e.g. SOC) in demonstrating compliance with the requirement. This would include all access management and data destruction requirements.
- Is the drafting team able to provide more detail on the distinction between “data” about BES Cyber Systems and “information” about BES Cyber Systems? Although the distinction is made in the definition, the distinction is not addressed in requirements or measures. ERCOT believes usability of the information is the key.
- ERCOT suggests Part 1.3 should be moved to CIP-004 with the proposed language.
- ERCOT suggests Part 1.5 should be moved to CIP-004 with the proposed language.
- ERCOT suggests Part 2.2 should note that separation of duties is only necessary when a vendor or other third-party is housing the information. This should not be required if the information is stored on-premises with the Responsible Entity.

- Part 3.1 is redundant to Part 1.2.
- As the drafting team is considering updating the standards, ERCOT suggests the existing standards evolve to align with industry security standards, such as NIST 800-53 / ISO 27001, and be more objective and outcome based.
- ERCOT suggests that the definition of BCSI should be modified to remove the examples. The definition allows for a risk-based approach to identifying BCSI, but the examples are being used as an authoritative list instead of a form of guidance. ERCOT believes the examples should be removed from the definition, and guidance written through other means.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; James McBee, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; Marcus Moor, Great Plains Energy - Kansas City Power and Light Co., 1, 3, 6, 5; - Douglas Webb, Group Name Westar-KCPL

Answer	Yes
Document Name	

Comment

Westar and Kansas City Power & Light Company, endorse Edison Electric Institute's (EEI) comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: James Mearns, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E recommends the SDT consider including the ability for an entity to use industry or federally approved certifications such as FedRAMP for CIP-011 R1, Part 1.4 in place of doing their own risk assessment.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Comments: ISO-NE commends the SDT for taking on the challenge to address BCSI compliance issues that existed even in the CIPv3 days. ISO-NE recommends that the SDT consider approaching the information security risks and protections on an objective basis instead of a prescriptive basis. The standard should require the parts/elements/criteria that must be included in a security risk assessment plan without prescribing solutions or technologies. As stated in the SAR, the standard should allow multiple methods for controlling access to BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 5, 3; Chris Gowder, Florida Municipal Power Agency, 6, 4, 5, 3; Dale Ray, Florida Municipal Power Agency, 6, 4, 5, 3; David Owens, Gainesville Regional Utilities, 1, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 5, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Angela Gaines - Portland General Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
MRO appreciates the efforts of the 2019-02 team over the past months. While there is good in the draft, the proposed language for CIP-011-3 Part 1.4 is too high level. Requiring a "Process to identify, assess, and mitigate risks…" offers no direction as to what risk considerations are a concern. *As discovered by the 2016-02 CIP SDT, objective based requirements seem to hit the mark when the requirement language guides the 'what', but not the 'how'. If 'mitigate the risk' language is used, the language should guide entities to address a minimum set of risk considerations. Risk considerations should include risk categories that are typical for the cloud environment, such as service level agreements, encryption (logical protections), data sovereignty, data transformations, and certifications.* *If left as written, the ERO enforcement of this objective based requirement will likely become equally open ended.*	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	
Document Name	
Comment	
CIP-011-3 R1.6. - Suggest a rewording of the requirement to "Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and that the Responsible Entityt determines is necessary for performing assigned work functions." CIP-011-3 R3.1 - This requirement is not needed if the term 'sanitization' is included in Part 1.2 as discussed in Q4. Any associated measures could be included there as well.	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE has the following additional comments: • Part 3.1 table header: should be revised from “BES Cyber Asset Reuse and Disposal” to “Cyber Asset Reuse and Disposal”, the applicable systems column contains EACMS, PACS, and PCAs as well. • Update the Applicable Systems columns in CIP-004-7 R4 (Parts 4.1-4.3) and R5 (Parts 5.1-5.4), to include PCA and Medium Impact BES Cyber Systems (versus Medium Impact BES Cyber Systems with External Routable Connectivity). Since CIP-011-3 Part 3.1 includes EACMS, PACS, and PCA, this change would align better CIP-004-7 better with CIP-011-3 as well as improve an overall security posture for access management and revocation.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon supports EEI's comments on behalf of Exelon Segments 1, 3, 5, and 6.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
The standards development team should draft separate requirements for cloud vs in house BCSI.	
Likes 0	
Dislikes 0	
Response	
Kathryn Tackett - NiSource - Northern Indiana Public Service Co. - 5	
Answer	
Document Name	
Comment	
See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 3	
Answer	
Document Name	
Comment	

See Steven Toosevich's comments.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-02 BES Cyber System Information Access Management

Summary Response to Comments

Background

Project 2019-02 enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI). In addition, the project
seeks to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

The standard drafting team (SDT) revised Reliability Standards CIP-004 and CIP-011 and reviewed the Glossary of Terms Used in NERC Reliability Standards pertaining to requirements addressing BCSI. The 45-day comment period was December 20, 2019 through February 3, 2020. There were 91 sets of responses, including comments from approximately 209 different people from approximately 131 companies representing 10 of the Industry Segments as shown in the table on the following pages. Based on these comments, the SDT has made proposed revisions to CIP-004 and CIP-011. Summary responses have been developed to address the comments.

Question 1

The proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Summary

A comment states the proposed changes add PCAs as applicable systems, which by definition do not contain BCSI. It seems that this addition is outside of the SAR and it would be helpful for the SDT to describe how adding this "clarifies the protections expected when utilizing third-party solutions".

Response

Thank you for your comments. The SDT does not agree that PCAs by definition are exempt from containing BCSI. Each Registered Entity's system and implementation is different, and there is nothing that precludes a PCA from containing BCSI. As one example, an entity may have a vulnerability scanner located within its ESP and this scanner may contain security configuration, network settings, enabled ports and services, and vulnerability status information of the BCAs. As another example, an entity may choose to implement a file server inside the ESP to store information like but not limited to ESP diagrams,

response or recovery plans, system backups of conjuration files etc. which could be considered BCSI. That said, the SDT considered industry feedback and removed PCA from the Applicable Systems column.

Summary
Several commenters state that the removal of the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems in CIP-011-3 R1.1 as currently provided in CIP-004-6 R4.1 expands the scope of all subsequent parts of Requirements R1 and R2.

Response
Thank you for your comments. The SDT has considered these comments and has reverted the applicability to include ERC.

Summary
Several commenters believe a more effective approach would be to clearly state security objectives instead of prescriptive requirements.

Response
Thank you for your comments. The SDT agrees that objective requirements provide maximum flexibility to allow an entity to determine how to comply with the objective. The SDT was mindful to strike an appropriate balance between high level security objectives and enough detail to assure the expectations are clear.

Summary
Some commenters recommend removing "System information pertaining to" from the "Applicability" column of the Requirement Table and the applicability should be limited to BCSI.

Response
Thank you for your comments. The SDT adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1.

Summary
Some commenters believe clarification is needed in CIP-011-3 Requirement R1 Part 1.1 to identify BCSI storage locations as the requirement would create difficulty in identifying third-party storage locations or that it should be removed.

Response
Thank you for your comments. The SDT has adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1 and maintained the focus on the BCSI itself instead of storage locations. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location.

Summary
A comment stated that "method" should not be replaced with the term "process." A "method" for identification allows Responsible Entities to provide guidelines and criteria to their personnel to aid in identification of BCSI without requiring a pre-defined series of steps or action (e.g., a process) to be utilized by such personnel in the identification. This distinction is critical because a process can be high-level and – thereby – provide significant variability in what is identified as BCSI whereas a method provides personnel with enough guidance to provide consistency relative to BCSI identification without being overly prescriptive regarding how such identification is accomplished.

Response
Thank you for your comments. The SDT agrees with industry comments and has adjusted the requirement language to make use of the word "methods" instead of "process".

Summary
A comment stated that the SDT should create a new term "BCSI Repository"

Response
Thank you for your comments. The SDT considered industry comments to establish a new term for "BCSI Repository" because it is too prescriptive as to how an entity would have to meet the directive. For this reason, the SDT maintained the focus on the BCSI itself instead of storage locations or repositories. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location or repositories.

Summary
Registered entities would have difficulty proving the granting and removal of access to BCSI as contemplated in the proposed draft for CIP-004-7. As an alternative, EEI suggests using the BCSI Repository definition shown above, and revising proposed CIP-004-7 to require registered entities to prove access and removal of access to a BCSI Repository.

Response
Thank you for your comments. The SDT has revised the CIP-011-3 and CIP-004-7 requirements in order to retain backward compatibility with existing requirements where BCSI protections are applied to storage repositories. This should allow registered entities to prove access and removal of access to a BCSI Repository.

Question 2

The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

Summary

Several commenters state that Requirements related to access management should remain in CIP-004.

Response
Thank you for your comments. In response to the large number of comments received related to moving BCSI access management requirements from CIP-004 to CIP-011, the BCSI SDT has move the BCSI access management requirements back into CIP-004 in a newly created CIP-004 Requirement 6.

Summary
Switching from access controls on repositories to access controls on BCSI

Response
Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to implement.

Summary
Some commenters disagree with dropping the qualifying language "with ERC" from the applicability of Medium Impact BES Cyber Systems from CIP-004-6 Requirement R4 Part 4.1 when moved to CIP-011-3 Requirement R1 Part R1.3. This deletion greatly expands the scope of this requirement, and may have created a situation where Responsible Entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards.

Response
Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with facilities containing medium impact BES Cyber Systems that do not have External Routable Connectivity to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary
A comment states that there is not minimal effort to meet the proposed obligations due to the addition of PCAs.

Response
Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with Protected Cyber Assets to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary
Concerns with adding vendor risk assessments

Response
Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment.

Summary
Some commenters noted the proposed changes may create a situation where responsible entities could be subject to multiple compliance violations based on a single action due to overlapping obligations in the CIP Standards. The proposed changes in CIP-011-3 also introduce a new complication, that of having to maintain similar access authorization, revocation and control measures as that in CIP-004-7. This could create a situation whereby a single deficiency in an entity's access management program could lead to potential non-compliance with two NERC standards at the same time.

Response
Thank you for your comments. The SDT moved the BCSI access authorization and revocation requirements from CIP-011-3 back into CIP-004-7 to eliminate the risk of potential non-compliance with two NERC standards at the same time.

Summary
A commenter does not agree with draft revisions as one of the fundamental concepts of CIP-004 Requirement R4 Part 4.1.3 that was lost in the proposed transition to CIP-011 Requirement R1 Part 1.3 is the difference between authorizing access to *BCSI storage locations,* which is a discrete and finite object that can be monitored and audited (the current CIP-004 approach), while the new CIP-011 approach is *access to BCSI* wherever and however it exists inside or outside of its storage locations (i.e. a hardcopy of a network diagram in a company truck). This fundamental change has made the requirement unmeasurable and non-auditable.

Response
Thank you for your comments. The SDT believes that this concern has been addressed through the revisions made to CIP-004-7 R6 and CIP-011 R1 Part 1.2 regarding the protection and the secure handling of BCSI, regardless of whether it is within a storage location or not.

Summary
A commenter disagrees with the addition of "disposal" to CIP-011 Requirement R1 Part 1.2.

Response
Thank you for your comments. The SDT has removed the term "disposal" from CIP-011 Requirement R1 Part 1.2.

Question 3

The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

Summary
Concerns with adding vendor risk assessments

Response
Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment.

Summary
A comment states it would be better to focus efforts on Requirements that do not hinder the use of other solutions while allowing for the development of access control programs by Responsible Entities that address risk posed to the industry.

Response
Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented

Summary
A comment states new R2 requirements are too prescriptive and cannot be prudently applied across all BCSI storage solutions and they limit the ability for the entity to manage their own compliance.

Response
Thank you for your comments. The SDT has removed R2 from the standard and incorporated it into R1.4 for clarity.

Summary
Some commenter noted the requirements as written do not clearly reflect an approach to expand information storage solutions or security technologies

Response
Thank you for your comments. The SDT thanks you for your comments. The language has been modified to allow RE's to be able to expand information storage solutions specific to third parties.

Summary
A comment suggests the team focus on the approach taken in the current NERC CMEP Guidance document in addressing the issue

Response

Thank you for your comments. The CMEP guidance has been used to directly develop the new language for controlling access to BCSI and protecting BCSI.

Question 4

The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms "obtain" and "use" in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

Summary

Commenters Agree with terms "obtain" and "use;" however, more explanation is needed within the requirement or guidelines. The drafting team has referred to the CMEP BCSI practice guide. We recommend defining "BCSI Access" in the NERC Glossary of Terms per the practice guide.

Response

Thank you for your comments. The SDT has taken the approach to refine the concept of access to BCSI through the ability to "obtain" and "use" within the CIP-011 Implementation Guidance, rather than the NERC Glossary of Terms.

Summary

A comment states while this approach is better than previous approaches, there is still a need for security technology vendor service providers to have access and use of BCSI.

Response

Thank you for your comments. The SDT acknowledges the potential need for vendor service providers to have the ability to "obtain" and "use" BCSI within their service model. The SDT Believes that the revisions made to CIP-011-3 R1 Parts 1.3 and 1.4 provide the Responsible Entity with the appropriate compliance framework when engaging vendor services to store, utilize, or analyze BCSI.

Question 5

The SDT is proposing to have BCSI in the "Applicability" column. Do you agree that this provides better clarity on the focus of the requirements?

Summary

Several commenters stated that the revisions expanded beyond the scope of the SAR. The commenters disagree with absence of ERC for Medium Impact BES Cyber Systems and the additions of PCAs, and want exemption for BCS, EACMS and PACS as BCSI repositories.

Response

Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements where Applicable Systems scopes Medium impact BES Cyber Systems with ERC, removed PCA from the Applicable Systems column, and decided to continue to scope the proposed modifications to align with the SAR objectives to focus on the BCSI.

Summary
Several commenters requested that the "Applicability" column be changed back to "Applicable Systems". Commenters stated it creates ambiguity and inconsistency and recommends the SDT use requirement language to scope to BCSI.

Response
Thank you for your comments. The SDT removed the undefined language in favor of using the defined term BCSI to address concerns about ambiguity. The SDT adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1.

Summary
A couple of commenters noted confusion of the "applicability" as the column header with Section 4 applicability and answered in a manner that calls out a perceived issue to consider Section 4 when auditing CIP-002 citing NERC's March 1, 2019 Standards Process Manual Appendix 3A page 6 last paragraph "The only mandatory and enforceable components of a Reliability Standard are the (1) Applicability, (2) Requirements, and (3) effective dates."

Response
Thank you for your comment. The SDT was referring to the use of the word "Applicability" in the Table Requirement Parts and the use of BCSI within that table column and not Section 4. Applicability of the CIP-011 Standard and the scope of the 2019-02 SAR. CIP-002 is not in scope for this SAR and the 2019-02 SDT cannot speak to the oversight practices for Section 4 Applicability related to CIP-002."

Question 6

The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

Summary
Several commenters state that the vendor risk assessment overlaps with CIP 013 required assessment and likely belongs in CIP-013.

Response
Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment.

Summary
Some commenters note the application and language of the key control requirement is unclear in CIP-011 Requirement R2 Part 2.1.

Response
Thank you for your comments. The specific requirement related to key control has been removed.

Summary
Some commenters note the application and language of the separation of duties requirement is unclear.

Response
Thank you for your comments. The specific requirement related to the separation of duties has been removed.

Summary
Some commenters note responsible entities should have an exemption for regulators regarding these requirements.

Response
Thank you for your comments. Language has been added to the requirements to clarify that it is when a vendor's services are used that certain requirements must be met.

Summary
Several commenters state that the vendor risk assessment lacks a clear value proposition.

Response
Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent. Specifically, the assessment is not about the vendor, but instead is an assessment of the vendor's technical environment. Language has been added to the requirements to clarify that it is when a vendor's services are used that certain requirements must be met.

This requirement ensures that prior to BCSI entering a vendor's environment, the Responsible Entity is well informed regarding the vendor's environment and controls and should influence what if any varying controls offered by a vendor are utilized or may influence the Responsible Entity to use technical mechanisms (see CIP-0011 R2) that the Responsible Entity has more control over.

Summary
Some commenters note that these requirements may work better as guidance documents.

Response
Thank you for your comments. The SDT has made numerous modifications to ensure the requirements are clear.

Summary
Commenters voiced concern that the vendor risk assessment requires mitigation; especially since CIP-013 doesn't require mitigation.

Response

Thank you for your comments. The SDT made a number of updates to CIP-011 Requirement 1.3 to clarify our intent and the requirements for mitigation have been removed.

Summary
Some commenters noted that CIP-011 Requirement R2 could potentially be eliminated.

Response
Thank you for your comments. The SDT has clarified the intent of CIP-011 Requirement 2. This requirement is critical to ensuring the security of BCSI when utilizing a vendor's services.

Question 7

The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

Summary
Some commenters note the language proposed by the SDT is too narrow and prescriptive.

Response
Thank you for your comments. The SDT has made changes to the requirements to allow for more flexibility in the use of future technologies. The requirements around key controls and separation of duties have been added to the measures and are no longer part of the requirements language.

Summary
Some commenters note this change expands the scope of these requirements beyond the original BCSI access requirements in CIP-004-6 R4 and R5

Response
Thank you for your comments. The SDT has purposefully separated BCSI access into CIP-004 and identifying and protecting BCSI in CIP-011.

Question 8

The SDT is proposing a new "key management" set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

Summary
Some comments note encryption should not be the only acceptable method of protecting BCSI; methods should be based on risk.

Response
Thank you for your comments. The SDT agrees with the submitters comment and has revised CIP-011-3 R1 Part 1.4 to include "one or more documented electronic technical mechanisms to protect BCSI" to allow the Responsible Entity more flexibility when considering the risk of implementation.

Summary
Some comments note the requirement is unclear if this is an electronic key or a physical key. Adding electronic key controls as prescribed by the Standard is unnecessarily burdensome for entities.

Response
The SDT has remove the specific "key management" requirement language from CIP-011-3 and replaced it with a more generic "one or more documented electronic technical mechanisms to protect BCSI" within CIP-011-3 R1 Part 1.4.

Question 9

The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or "hardware" storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

Summary
Several commenters stated the team should continue focusing on access controls to repositories.

Response
Thank you for your comments. The SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented.

Summary
Some commenters state that the approach as written may prevent using cloud services and may require physical protections for electronic repositories, which would preclude using cloud services.

Response
Thank you for your comments. The SDT has drafted numerous updates to clarify our intent and specifically allow Responsible Entities to leverage cloud services. Specifically, the modification to CIP-004 Requirement 6 which now focuses on the provisioning of access, and the modification to CIP-011 Requirement 1.2 which now focuses on the prevention of unauthorized access should clarify that physical access to electronic repositories is not access to BCSI. Additionally, CIP-011 Requirement 2 specifically speaks to controlling unauthorized logical access, which should also address this concern.

Summary
A commenter stated the additional controls may not have offsetting additional value to reliability and/or security.

Response

Thank you for your comments. The number and type of controls required has been streamlined and clarified.

Summary
Several commenters asserted that adding the non-ERC facilities to the access management expands the scope.

Response
Thank you for your comments. The SDT recognizes that adding access management requirements for BCSI associated with facilities containing medium impact BES Cyber Systems that do not have External Routable Connectivity to the CIP-004 BCSI access management requirements is an increase in scope beyond the scope of the SAR. Therefore, this addition has been removed.

Summary
Commenters expressed the approach isn't backwards compatible.

Response
Thank you for your comments. The BCSI SDT has drafted a number of updates to the requirements to clarify the drafting team's intent. Primarily, the updates related to the provisioning of access in the newly created CIP-004 Requirement 6 address this concern by clarifying that it is the provisioning of an access privilege that allows ongoing access to BCSI that must be controlled, and not simply the ability to view BCSI that is made available. This clarification allows entities with access management programs focused on BCSI repositories to continue leveraging those programs, while also allowing for programs that focus on individual pieces of BCSI to be implemented.

Question 10

The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

Summary
Several commenter maintain that CIP-004-6 already effectively addresses access controls for BCSI stored by responsible entities

Response
Thank you for your comments. In response to the large number of comments received related to moving BCSI access management requirements from CIP-004 to CIP-011, the BCSI SDT has move the BCSI access management requirements back into CIP-004 in a newly created CIP-004 Requirement 6.

Summary
A comment recommended the SDT create Part in CIP-004 for protections where third party cloud-based services are used.

Response
Thank you for your comments. The SDT has created a new CIP-004 Requirement 6 specifically for BCSI access management and it is applicable to all BCSI access, including where third party cloud-based services are used.

Summary
A few commenters noted that it creates impossibility for compliance of individual vendor staff.

Response
Thank you for your comments. By incorporating the BCSI access concepts of the **ERO Enterprise CMEP Practice Guide***: BES Cyber System Information* into the revised CIP-011 standard language, the SDT believes that they have provided a vehicle for industry to comply with CIP-004 BCSI access requirements when using a 3rd party cloud vendor.

Question 11

The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

Summary
Several commenters expressed concern of and expansion of scope to Mediums without ERC, contending BCS w/out ERC are lower risk, expansion is burdensome and not justified, and the approach does not conform to the risk-based approach that the ERO has been striving toward.

Response
Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements where Applicable Systems scopes Medium impact BES Cyber Systems with ERC.

Summary
Several commenters cannot support expansion to PCA. PCAs are lower risk, expansion is burdensome and not justified, and the approach does not conform to the risk-based approach that the ERO has been striving toward.

Response
Thank you for your comments. The SDT does not agree that PCAs by definition are exempt from containing BCSI. Each Registered Entity's system and implementation is different, and there is nothing that precludes a PCA from containing BCSI. As one example, an entity may have a vulnerability scanner located within its ESP and this scanner may contain security configuration, network settings, enabled ports and services, and vulnerability status information of the BCAs. As another example, an entity may choose to implement a file server inside the ESP to store information like but not limited to ESP diagrams,

response or recovery plans, system backups of conjuration files etc. which could be considered BCSI. That said, the SDT considered industry feedback and removed PCA from the Applicable Systems column.

Summary
Several commenters maintain the proposed modifications are outside the scope of the SAR and do not address the SAR specifically, and should be limited to use of cloud services for BCSI and requirements to permit cloud use.

Response
Thank you for your comments. The SDT considered industry feedback and has scoped the proposed modifications to align with the SAR objectives by adjusting the requirement language to focus on "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI…"

Summary
Several commenters maintain the change in applicability to BCSI greatly expands scope to all BCSI instead of just the repositories, and is not backwards compatible with storage locations

Response
Thank you for your comments. The SDT considered industry feedback and moved forward with changing applicability to BCSI within the Requirement language. The concept that not all BCSI is in scope today is at odds with the original intent, and this adjustment brings the requirements into alignment with the security objective. The SDT has adjusted the applicability to read BCSI as identified in Requirement R1 Part 1.1, and maintained the focus on the BCSI itself instead of storage locations. This change is fully backwards compatible and does not preclude an entity from identifying and using storage locations, while enabling entities who are ready to use of service provider technologies that are capable of applying protections to the BCSI regardless of storage location.

Summary
Several commenters maintain the "System information pertaining to" language is unclear.

Response
Thank you for your comments. Thank you for your comment. The SDT removed the undefined language in favor of using the defined term BCSI. The Applicability now reads, "BCSI as identified in Requirement R1 Part 1.1"

Summary
Several commenters maintain the proposed modifications create double jeopardy concern between CIP-011 and CIP-004.

Response
Thank you for your comments. The SDT considered industry feedback and moved the proposed CIP-011 requirements back to the original CIP-004 requirements to address this concern.

Summary
Several commenters agree a PCA may contain BCSI.

Response
Thank you for your comment. The SDT appreciates your support for PCA in the Applicable Systems column. Based on industry opposition to this change, the SDT removed PCA and focused the Requirement on BCSI.

Question 12

In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

Summary
Some commenters stated that key management would result in increased costs for utilities that do not currently have key management programs in place.

Response
Thank you for your comments. The SDT has remove the specific "key management" requirement language from CIP-011-3 and replaced it with a more generic "one or more documented electronic technical mechanisms to protect BCSI" within CIP-011-3 R1 Part 1.4.

Summary
Some commenters requested to consider creating an industry standard or leveraging existing federal standards for vendors for certifications.

Response
Thank you for your comments. The SDT acknowledges the ability to leverage certification models such as The Federal Risk and Authorization Management Program (FedRAMP) would provide industry with a streamlined and cost-effective way to engage vendor services used to store, utilize, or analyze BCSI. However, this model is not feasible since NERC and Regional Entities are currently not able to rely on the work of others in lieu of direct compliance evidence. Resolving this broader topic on certification models is beyond the scope of the Project 2019-02 SAR.

Summary
Several commenters indicated that the shift from protecting repository to information level increases both cost and effort with no additional security, compliance, reliability or operational benefits.

Response
Thank you for your comments. The SDT has revised the CIP-011-3 requirements in order to retain backward compatibility with existing CIP-011-2 requirements where BCSI protections are applied to storage repositories. This should alleviate concerns where cost is an issue when protecting BCSI at the information level.

Summary
Some commenters stated that doing periodic or time-based risk assessments do not return the value especially when the risks are low and suggested entities could have the flexibility of conducting vendor risk assessment based on criteria, such as their risk management plan for high, medium and low risk posture.

Response
Thank you for your comments. The SDT believes that revisions made to CIP011-3 R1 Part 1.3 allow the entity to implement a risk assessment methodology commensurate with the type of vendor services utilized to store, utilize, or analyze BCSI.

Question 13

Do you have any other general recommendations/considerations for the drafting team?

Summary
Several commenters state that many of the proposed changes are not in the scope of the approved SAR and are too rigid.

Response
Thank you for your comments. The SDT made several updates to the CIP-011 and CIP-004 requirements and now believe that these revisions are in line with the scope of the SAR and offer more flexibility in their implementation.

Summary
Several commenters state they prefer to see goal and objective based requirements, not prescriptive.

Response
Thank you for your comments. The SDT has attempted to make the revisions to the requirements more goal and objective based.

Summary
Several commenters state the risk identification and assessment portion of the requirement overlaps with CIP-013.

Response
Thank you for your comments. The SDT worked with members from the Project 2019-03 Cyber Security Supply Chain Risks (CIP-013) drafting team to revise wording and add clarity in order to eliminate the perceived overlap between the risk assessments prescribed in the CIP-011 and CIP-013 standards.

Summary
Several commenters state that by eliminating the exclusion of Medium Impact BES Cyber Systems without External Routable Connectivity (ERC), the drafting team is exceeding the SAR.

Response

Thank you for your comments. The SDT has reinstated the Medium Impact BES Cyber Systems without External Routable Connectivity (ERC) exclusion into the CIP-004 R6 BCSI Access requirement language.

Summary
Some commenters note that Applicability should include "BES Cyber System Information stored in vendor managed electronic BCSI Repositories" (Various requirements) /SDT should draft separate requirements for cloud vs in house BCSI.

Response
Thank you for your comments. The SDT believes that it has added clarification in the CIP-011 requirements that identify those that are only applicable when the Responsible Entity uses vendor services to store, utilize, or analyze BCSI.

Summary
Commenters recommend that the scope of the standards team consider leveraging standards such as Fedramp to justify the use of cloud services.

Response
Thank you for your comments. The SDT added revised the Measures language within the CIP-011 R1.3 requirement to include Vendor certifications (i.e. Fedramp) as a potential way to confirm compliance with the CIP-011 R1.3 requirement (Risk Assessment).

Summary
CIP-011-3 R2 Part 2.1 introduces nine terms in its sub-parts 2.1.1 through 2.1.9. These nine terms are not further discussed or defined.

Response
Thank you for your comments. The SDT has deleted Requirement R2.

Summary
Several commenters state the changes to the standard do not provide any clarification regarding the definition of BCSI. Entities will need at least 24 months to achieve compliance with these new requirements. Without splitting EACMS into EACS and EAMS, the issue of third-party analysis systems is not addressed but is included in the SAR.

Response
Thank you for your comments. Revisions to the definition of BCSI within the NERC Glossary of Terms is not in the scope of the SAR. By removing some of the revisions made to CIP-004 and CIP-011 as part of the first comment/ballot posting, the SDT believes that entities can more reasonably achieve compliance within the 18-month timeframe prescribed as part of the Implementation Plan.

Summary
Commenters state that eliminate is extremely strong wording.

Response
Thank you for your comments. The word "eliminate" was removed from the revised CIP-011 requirement language.

Summary
Several commenters state it would be better to continue focusing authorization for access to storage locations and make that more robust; and Focus on Storage location BESCSI repositories.

Response
Thank you for your comments. The SDT believes that the proposed revisions to CIP-004 and CIP-011 support backward compatibility with prior versions that require controlling and authorizing access to BCSI storage locations. If an Entity wishes to continue in that manner, the revised standards would allow that.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through February 3, 2020
Ballot Pools Forming through January 20, 2020

Now Available

A 45-day formal comment period for **Project 2019-02 BES Cyber System Information Access Management** is open through **8 p.m. Eastern, Monday, February 3, 2020.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Linda Jenkins. 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. - 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 Standards and Implementation Plan, along with non-binding polls for each associated Violation Risk Factors and Violation Severity Levels, will be conducted **January 24 – February 3, 2020.**

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

For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 IN 1 ST
Voting Start Date: 1/24/2020 12:01:00 AM
Voting End Date: 2/3/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 256
Total Ballot Pool: 279
Quorum: 91.76
Quorum Established Date: 2/3/2020 3:22:12 PM
Weighted Segment Value: 15.37

Actions

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	80	1	9	0.129	61	0.871	0	3	7
Segment: 2	2	0.2	0	0	2	0.2	0	0	0
Segment: 3	60	1	7	0.125	49	0.875	1	0	3
Segment: 4	17	1	3	0.176	14	0.824	0	0	0
Segment: 5	69	1	11	0.196	45	0.804	0	2	11
Segment: 6	44	1	5	0.119	37	0.881	0	0	2
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	1	0.1	2	0.2	0	3	0
Totals:	279	5.5	36	0.846	210	4.654	1	9	23

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Third-Party Comments
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Third-Party Comments
6	Western Area Power Administration	Rosemary Jones		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments

					Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A

1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Negative	Third-Party Comments
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted

5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen	Affirmative	N/A
3	Lakeland Electric	Patricia Boody	Negative	No Comment Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough	Negative	Comments Submitted
1	Manitoba Hydro	Bruce Reimer	Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley	Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao	Negative	Comments Submitted
3	Manitoba Hydro	Karim Abdel-Hadi	Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas	Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Kjersti Drott	Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Richard Schlottmann	Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Third-Party Comments
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz	Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen	Negative	Third-Party Comments
5	Black Hills Corporation - Black Hills Power	Don Stahl	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
				Comments

3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	Negative	Submitted
6	New York Power Authority	Thomas Savin	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price	Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Third-Party Comments
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Marcus Moor	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Negative	Comments Submitted
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Donald Lynd	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta	Negative	Third-Party Comments

3	Nebraska Public Power District	Tony Eddleman	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey	Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Negative	Third-Party Comments
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi	None	N/A
6	Los Angeles Department of Water and Power	Anton Vu	Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck	Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy	Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson	Negative	Third-Party Comments
5	JEA	John Babik	Negative	Third-Party Comments
				Comments

2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Third-Party Comments
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		Negative	Third-Party Comments
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted

5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Kristine Ward		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted

6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	None	N/A
3	City Utilities of Springfield, Missouri	Scott Williams	Negative	Third-Party Comments
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Dwayne Parker	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Negative	Third-Party Comments
1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel	None	N/A
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong	Negative	Comments Submitted
5	AEP	Thomas Foltz	Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Abstain	N/A
		W. Dwayne		

3	Austin Energy	Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	David Weber	Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson	None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Barry Lawson	Negative	Comments Submitted
4	Arkansas Electric Cooperative Corporation	Alice Wright	Negative	Third-Party Comments
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	Negative	Third-Party Comments
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	Negative	Third-Party Comments
3	Arkansas Electric Cooperative Corporation	Mark Gann	Negative	Third-Party Comments
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Ben Engelby	Negative	Third-Party Comments
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	Negative	Comments Submitted
5	SunPower	Bradley Collard	Negative	Comments Submitted
5	SunPower	Bradley Collard	None	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 IN 1 ST
Voting Start Date: 1/24/2020 12:01:00 AM
Voting End Date: 2/3/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 257
Total Ballot Pool: 278
Quorum: 92.45
Quorum Established Date: 2/3/2020 3:22:21 PM
Weighted Segment Value: 13.04

Actions

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	80	1	7	0.1	63	0.9	0	3	7
Segment: 2	2	0.2	0	0	2	0.2	0	0	0
Segment: 3	59	1	6	0.105	51	0.895	0	0	2
Segment: 4	17	1	3	0.176	14	0.824	0	0	0
Segment: 5	69	1	8	0.14	49	0.86	0	2	10
Segment: 6	44	1	4	0.095	38	0.905	0	0	2
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	1	0.1	2	0.2	0	3	0
Totals:	278	5.5	29	0.717	219	4.783	0	9	21

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Third-Party Comments
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Third-Party Comments
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Moser		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Third-Party Comments
6	Western Area Power Administration	Rosemary Jones		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments

					Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
10	Midwest Reliability Organization	Russel Mountjoy		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments

1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Negative	Third-Party Comments
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		Negative	Third-Party Comments

5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
3	Manitoba Hydro	Karim Abdel-Hadi		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
5	Lakeland Electric	Becky Rinier		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Third-Party Comments
3	Eversource Energy	Sharon Flannery		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen		Negative	Third-Party Comments
5	Black Hills Corporation - Black Hills Power	Don Stahl		Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
					Comments

6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	Negative	Comments Submitted
6	New York Power Authority	Thomas Savin	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price	Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Third-Party Comments
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Marcus Moor	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Negative	Comments Submitted
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Donald Lynd	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Negative	Third-Party Comments

6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta	Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey	Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Negative	Third-Party Comments
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi	None	N/A
6	Los Angeles Department of Water and Power	Anton Vu	Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck	Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy	Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson	Negative	Third-Party Comments

5	JEA	John Babik		Negative	Third-Party Comments
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		Negative	Third-Party Comments
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted

5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Kristine Ward		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted

5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	None	N/A
3	City Utilities of Springfield, Missouri	Scott Williams	Negative	Third-Party Comments
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Dwayne Parker	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Negative	Third-Party Comments
1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong	Negative	Comments Submitted
5	AEP	Thomas Foltz	Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Negative	Comments Submitted
6	AEP - AEP Marketing	Yee Chou	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Abstain	N/A

3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	David Weber	Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson	None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Barry Lawson	Negative	Comments Submitted
4	Arkansas Electric Cooperative Corporation	Alice Wright	Negative	Third-Party Comments
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	Negative	Third-Party Comments
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	Negative	Third-Party Comments
3	Arkansas Electric Cooperative Corporation	Mark Gann	Negative	Third-Party Comments
5	Arkansas Electric Cooperative Corporation	Adrian Harris	Negative	Third-Party Comments
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Ben Engelby	Negative	Third-Party Comments
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	Negative	Comments Submitted
5	SunPower	Bradley Collard	Negative	Comments Submitted
5	SunPower	Bradley Collard	None	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management Implementation Plan IN 1 OT
Voting Start Date: 1/24/2020 12:01:00 AM
Voting End Date: 2/3/2020 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 250
Total Ballot Pool: 273
Quorum: 91.58
Quorum Established Date: 2/3/2020 3:31:38 PM
Weighted Segment Value: 22.3

Actions

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	78	1	11	0.175	52	0.825	0	8	7
Segment: 2	2	0.1	0	0	1	0.1	0	1	0
Segment: 3	58	1	11	0.204	43	0.796	1	1	2
Segment: 4	17	1	3	0.231	10	0.769	0	3	1
Segment: 5	67	1	13	0.245	40	0.755	0	4	10
Segment: 6	44	1	6	0.15	34	0.85	0	1	3
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	2	0.2	1	0.1	0	3	0
Totals:	273	5.4	46	1.204	181	4.196	1	22	23

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Third-Party Comments
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
					Third-Party

1	National Grid USA	Michael Jones		Negative	Comments
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
6	Western Area Power Administration	Rosemary Jones		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted

1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted

1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	No Comment Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer		Negative	Comments Submitted

3	Georgia System Operations Corporation	Scott McGough	Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley	Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Tony Skourtas	Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Kjersti Drott	Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Third-Party Comments
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Wes Wingen	Negative	Third-Party Comments
5	Black Hills Corporation - Black Hills Power	Don Stahl	Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	Negative	Comments Submitted
6	New York Power Authority	Thomas Savin	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price	Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Third-Party Comments
				Comments

3	Westar Energy	Bryan Taggart	Negative	Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Marcus Moor	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Negative	Comments Submitted
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	Donald Lynd	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Negative	Third-Party Comments
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta	Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey	Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A

5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	Negative	Third-Party Comments
6	Portland General Electric Co.	Daniel Mason	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi	None	N/A
6	Los Angeles Department of Water and Power	Anton Vu	Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck	Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy	Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson	Affirmative	N/A
5	JEA	John Babik	Negative	Third-Party Comments
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason	Abstain	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke	Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff	None	N/A
6	Imperial Irrigation District	Diana Torres	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse	Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell	Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry	Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding	Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein	None	N/A
1	NB Power Corporation	Nurul Abser	Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea	Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican	Terry Harbour	Negative	Comments

	Energy Co.				Submitted
5	Hydro-Qu?bec Production	Carl Pineault		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		Negative	Third-Party Comments
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted

5	Choctaw Generation Limited Partnership, LLLP	Rob Watson	None	N/A
3	Seminole Electric Cooperative, Inc.	Kristine Ward	Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead	Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender	Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer	Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal	None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield	Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert	Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra	Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Negative	Comments Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	None	N/A
3	City Utilities of Springfield, Missouri	Scott Williams	Negative	Third-Party Comments
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Dwayne Parker	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Negative	Third-Party Comments

1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong	Negative	Comments Submitted
5	AEP	Thomas Foltz	Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Abstain	N/A
6	AEP - AEP Marketing	Yee Chou	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Abstain	N/A
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	David Weber	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Paul McCurley	None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright	Negative	Third-Party Comments
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	Negative	Third-Party Comments
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	Negative	Third-Party Comments
3	Arkansas Electric Cooperative Corporation	Mark Gann	Negative	Third-Party Comments
				Third-Party

5	Arkansas Electric Cooperative Corporation	Adrian Harris	Negative	Comments
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Ben Engelby	Negative	Third-Party Comments
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	Affirmative	N/A
5	SunPower	Bradley Collard	Negative	Comments Submitted
5	SunPower	Bradley Collard	None	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 Non-Binding Poll IN 1 NB
Voting Start Date: 1/24/2020 12:01:00 AM
Voting End Date: 2/3/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 232
Total Ballot Pool: 262
Quorum: 88.55
Quorum Established Date: 2/3/2020 4:51:25 PM
Weighted Segment Value: 18.88

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	73	1	8	0.145	47	0.855	10	8
Segment: 2	2	0.2	0	0	2	0.2	0	0
Segment: 3	59	1	10	0.204	39	0.796	6	4
Segment: 4	14	1	3	0.25	9	0.75	2	0
Segment: 5	64	1	10	0.227	34	0.773	8	12
Segment: 6	43	1	5	0.156	27	0.844	5	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.2	1	0.1	1	0.1	4	0
Totals:	262	5.4	37	1.083	159	4.317	36	30

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Abstain	N/A

1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Vivian Moser		Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted
6	Western Area Power Administration	Rosemary Jones		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted

5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
					Comments

3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted

3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz	Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen	Negative	Comments Submitted
5	Black Hills Corporation - Black Hills Power	Don Stahl	Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	Negative	Comments Submitted
6	New York Power Authority	Thomas Savin	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price	Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Negative	Comments Submitted
6	Muscatine Power and Water	Nick Burns	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Marcus Moor	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted

5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Negative	Comments Submitted
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
1	CMS Energy - Consumers Energy Company	Donald Lynd	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger	Negative	Comments Submitted
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted

3	BC Hydro and Power Authority	Hootan Jarollahi		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
5	JEA	John Babik		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		Negative	Comments Submitted
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	None	N/A

1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments

				Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	None	N/A
3	City Utilities of Springfield, Missouri	Scott Williams	Negative	Comments Submitted
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Dwayne Parker	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday	None	N/A
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong	Negative	Comments Submitted
5	AEP	Thomas Foltz	Abstain	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Abstain	N/A
6	AEP - AEP Marketing	Yee Chou	Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski	Abstain	N/A
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	David Weber	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	None	N/A
8	Florida Reliability Coordinating Council –	Vince Ordax	Abstain	N/A

	Member Services Division			
3	AEP	Kent Feliks	Abstain	N/A
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	Negative	Comments Submitted
5	Arkansas Electric Cooperative Corporation	Adrian Harris	Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Ben Engelby	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	Affirmative	N/A
5	SunPower	Bradley Collard	Negative	Comments Submitted
5	SunPower	Bradley Collard	None	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 Non-Binding Poll IN 1 NB
Voting Start Date: 1/24/2020 12:01:00 AM
Voting End Date: 2/3/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 232
Total Ballot Pool: 263
Quorum: 88.21
Quorum Established Date: 2/3/2020 5:08:16 PM
Weighted Segment Value: 15.31

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	73	1	6	0.107	50	0.893	9	8
Segment: 2	2	0.2	0	0	2	0.2	0	0
Segment: 3	59	1	8	0.163	41	0.837	6	4
Segment: 4	14	1	3	0.25	9	0.75	2	0
Segment: 5	65	1	8	0.186	35	0.814	9	13
Segment: 6	43	1	4	0.125	28	0.875	5	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.2	1	0.1	1	0.1	4	0
Totals:	263	5.4	30	0.931	166	4.469	36	31

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Daniel Valle	Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted

1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Ayman Samaan		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Vivian Moser		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted
6	Western Area Power Administration	Rosemary Jones		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted

4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Chinedu Ochonogor		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A

6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Comments Submitted
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Patricia Boody		Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Negative	Comments Submitted

1	Tri-State G and T Association, Inc.	Kjersti Drott	Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz	Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen	Negative	Comments Submitted
5	Black Hills Corporation - Black Hills Power	Don Stahl	Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk	Negative	Comments Submitted
6	New York Power Authority	Thomas Savin	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price	Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Negative	Comments Submitted
6	Muscatine Power and Water	Nick Burns	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Negative	Comments Submitted

5	Great Plains Energy - Kansas City Power and Light Co.	Marcus Moor	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Negative	Comments Submitted
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
1	CMS Energy - Consumers Energy Company	Donald Lynd	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Negative	Comments Submitted
6	PSEG - PSEG Energy Resources and Trade LLC	Luiggi Beretta	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger	Negative	Comments Submitted
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Abstain	N/A

1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
5	JEA	John Babik		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
3	Imperial Irrigation District	Denise Sanchez		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted
3	Portland General Electric Co.	Dan Zollner		Negative	Comments Submitted
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A

5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	None	N/A
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments

				Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Negative	Comments Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	None	N/A
3	City Utilities of Springfield, Missouri	Scott Williams	Negative	Comments Submitted
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Dwayne Parker	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday	None	N/A
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Preston Walsh	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong	Negative	Comments Submitted
5	AEP	Thomas Foltz	Abstain	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Abstain	N/A
6	AEP - AEP Marketing	Yee Chou	Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski	Abstain	N/A
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Abstain	N/A

5	Seminole Electric Cooperative, Inc.	David Weber	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Abstain	N/A
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	Negative	Comments Submitted
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Ben Engelby	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	Affirmative	N/A
5	SunPower	Bradley Collard	Negative	Comments Submitted
5	SunPower	Bradley Collard	None	N/A

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-7

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

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

4.1.2.2. Each or 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. 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**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-004-7:

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-004-7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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" or "Applicability" column. The "Applicable Systems" column further defines 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-002-5.1 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.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.1	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated authorization records for provisioned access to BCSI based on need; or • List of authorized individuals

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.2	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all provisioned access to BCSI: 6.2.1. Is authorized; and 6.2.2. Is appropriate based on need, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, all of the following: • List of authorized individuals; and • List of individuals who have been provisioned access; and • List of privileges associated with the authorizations; and • List of privileges associated with the provisioned access; and • Dated documentation of the 15-calendar-month verification; and • Documented reconciliation actions, if any.
6.3	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 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:

- The 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 Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes: 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.4)			
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items Parts 6.1 through 6.3. (R6)	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

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

2. **Number:** CIP-004-7~~6~~

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~Special Protection System (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.**~~**4.1.5. Reliability Coordinator**

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~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 ~~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-004-~~6~~7:

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-004-~~6~~7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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" or "Applicability" column. The "Applicable Systems" column ~~to~~ further define~~s~~ 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-002-5.1 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.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~6~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~6~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~6~~7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and~~,~~ unescorted physical access in a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

~~CIP-004-6 Table R4 – Access Management Program~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~4.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~0. EACMS; and~~ ~~0. PACS~~	~~Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.~~	~~An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following:~~ ~~0. A dated listing of authorizations for BES Cyber System information;~~ ~~0. Any privileges associated with the authorizations; and~~ ~~0. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.~~

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~6~~7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

~~CIP-004-6 Table R5 — Access Revocation~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~0. EACMS; and~~ ~~0. PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~0. EACMS; and~~ ~~0. PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.~~	~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.~~

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 5.1~~ or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~6~~7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.~~4~~5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.1	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated authorization records for provisioned access to BCSI based on need; or • List of authorized individuals

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.2	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all provisioned access to BCSI: 6.2.1. Is authorized; and 6.2.2. Is appropriate based on need, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, all of the following: • List of authorized individuals; and • List of individuals who have been provisioned access; and • List of privileges associated with the authorizations; and • List of privileges associated with the provisioned access; and • Dated documentation of the 15-calendar-month verification; and • Documented reconciliation actions, if any.
6.3	BCSI associated with: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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.~~

~~1.3.~~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 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 E~~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~~ The ~~Responsible E~~applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible E~~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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. Compliance Monitoring and Assessment Processes: 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.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access~~,~~ or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were~~	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were~~	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage~~	~~incorrect or unnecessary. (4.4)~~	~~incorrect or unnecessary. (4.4)~~	incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~locations, privileges were incorrect or unnecessary. (4.4)~~			
R5	**Same Day Operations and Operations Planning**	**Medium**	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or ~~,~~ unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of the termination action. (5.3)~~ ~~OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4~~3~~) OR The Responsible	access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the~~	access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective~~	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.~~5~~4) OR The Responsible	~~termination action. (5.3)~~	~~date and time of the termination action. (5.3)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.~~5~~4)			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~6~~7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items Parts 6.1 through 6.3. (R6)	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~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:~~

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

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

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

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

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

~~Requirement R2:~~

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing~~

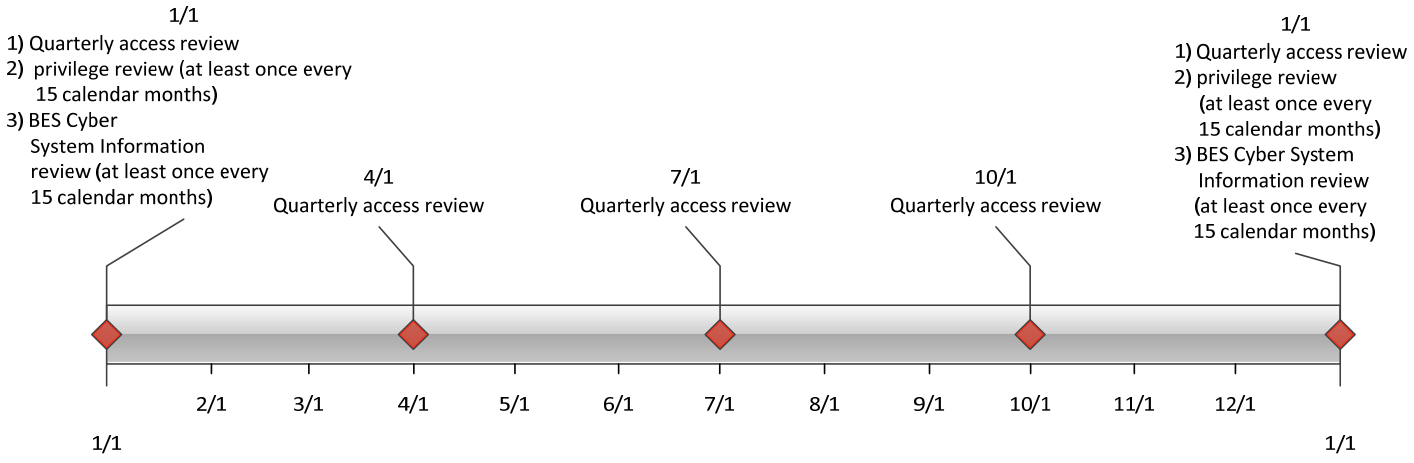
~~collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under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

~~Requirement R4:~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

~~**Rationale:**~~

~~During 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:**~~

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

~~**Rationale for Requirement R2:**~~

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

~~**Rationale for Requirement R3:**~~

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

~~**Rationale for Requirement R4:**~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.~~

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

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal comment period with additional ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-7

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

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

4.1.2.2. Each 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. 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:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

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-004-7.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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" or "Applicability" column. The "Applicable Systems" column ~~to~~ further defines 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-002-5.1 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.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in~~to~~ a Physical Security Perimeter.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.1	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated authorization records for provisioned access to BCSI based on need; or • List of authorized individuals

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicability**	**Requirements**	**Measures**
6.2	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all provisioned access to BCSI: 6.2.1. Is authorized; and 6.2.2. Is appropriate based on need, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, all of the following: • List of authorized individuals; and • List of individuals who have been provisioned access; and • List of privileges associated with the authorizations; and • List of privileges associated with the provisioned access; and • Dated documentation of the 15-calendar-month verification; and • Documented reconciliation actions, if any.
6.3	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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 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 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 E~~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~~ The ~~Responsible~~ applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible E~~ 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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes: 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.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.3)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances. (5.4)			
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI~~BES Cyber~~

Version	Date	Action	Change Tracking
			~~System Information~~.

~~*Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal or informal comment period with ballot	July 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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-011-3.

6. Background:

Standard CIP-011 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicable Systems" column further defines 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-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage location identified for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BCSI as identified in Part 1.1	Method(s) to protect and securely handle BCSI.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to protect and securely handle BCSI during its lifecycle, including: o Electronic mechanisms, o Physical mechanisms, o Technical mechanisms, or o Administrative mechanisms. • BCSI is handled in a manner consistent with the entity's documented procedure(s).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.3	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	Examples of acceptable evidence may include, but are not limited to, dated documentation of the following: • Implementation of the risk identification and assessment method(s) (1.3); • List of risk identification and assessment method(s) per vendor (1.3.1); • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4); • Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1); • Consideration made for data sovereignty, if any (1.3.1);

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
			• Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3); • Dated documentation of vendor's identity and access management program(1.3.2); and • Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	Examples of evidence may include, but are not limited to, dated documentation of the following: • Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]); • Evidence of implementation (e.g., configuration files, command output, architecture documents); and • Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 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:

- The 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 Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes: 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity did not implement one or more documented information protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal or informal comment period with ballot	July 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~2~~3

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-~~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. Effective Dates:

See Implementation Plan for CIP-011-~~2~~3.

6. Background:

Standard CIP-011 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicable Systems" column ~~to~~ further defines 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-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~2~~3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.1	BCSI pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify ~~information that meets the definition of BES Cyber System Information~~BCSI.	Examples of acceptable evidence include, but are not limited to, the following: • Documented method(s) to identify ~~BES Cyber System Information~~BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to ~~recognize~~ identify ~~BES Cyber System Information~~BCSI; or • ~~Repository or electronic and physical~~Storage location identified ~~designated~~ for housing ~~BES Cyber System Information~~BCSI in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicability~~le Systems~~**	**Requirements**	**Measures**
1.2	BCSI as identified in Part 1.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS; and~~ ~~PACS~~	~~Procedure~~Method(s) to ~~for protecting and~~protect and securely handle~~ing BES Cyber System Information~~BCSI~~, including storage, transit, and use~~.	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to protect and securely handle BCSI during its lifecycle, including: o Electronic mechanisms, o Physical mechanisms, o Technical mechanisms, or o Administrative mechanisms. ~~Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or~~ • ~~Records indicating that BES Cyber System Information~~BCSI is handled in a manner consistent with the entity's documented procedure(s).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.3	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	Examples of acceptable evidence may include, but are not limited to, dated documentation of the following: • Implementation of the risk identification and assessment method(s) (1.3); • List of risk identification and assessment method(s) per vendor (1.3.1); • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4); • Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1); • Consideration made for data sovereignty, if any (1.3.1);

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure
			• Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3); • Dated documentation of vendor's identity and access management program(1.3.2); and • Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirement**	**Measure**
1.4	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	Examples of evidence may include, but are not limited to, dated documentation of the following: • Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]); • Evidence of implementation (e.g., configuration files, command output, architecture documents); and • Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain ~~BES Cyber System Information~~BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI~~BES Cyber System Information~~, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI~~BES Cyber System Information~~ from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI~~BES Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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.~~

~~1.3.~~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 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~~ applicable ~~E~~entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority~~CEA~~ to retain specific evidence for a longer period of time as part of an investigation:

- ~~Each~~ The ~~Responsible~~ applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible~~ applicable ~~E~~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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. Compliance Monitoring and Assessment Processes: 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~

- ~~Self-Reporting~~
- ~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)	~~N/A~~ The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity ~~has~~ did not ~~documented or~~ implement~~ed~~ one or more ~~a~~ documented ~~BES Cyber System~~ information protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the BES Cyber Asset. (2.1)	the BES Cyber Asset. (2.2)	

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 information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.

~~**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:**~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.)~~

~~can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~Requirement R2:~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low-energy or high-energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

~~quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.~~

~~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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Rationale for Requirement R2:~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020

Anticipated Actions	Date
45-day formal or informal comment period with ballot	August 2020
10-day final ballot	September 2020
Board adoption	November 2020

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.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 ~~or~~ 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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-011-3.

6. Background:

Standard CIP-011 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" and "Applicability" Columns in Tables:
Each table has an "Applicable Systems" or "Applicability" column. The "Applicable~~ility~~ Systems" column further defines 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-002-5.1 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 information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	BCSI ~~System information~~ pertaining to: High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS~~; and~~ ~~3. PCA~~ Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS~~; and~~ ~~3. PCA~~	Method(s)~~Process(es)~~ to identify BCSI.~~information that meets the definition of BES Cyber System Information and identify applicable BES Cyber System Information storage locations.~~	Examples of acceptable evidence include, but are not limited to, the following: • Documented ~~process(es)~~method(s) to identify ~~BES Cyber System Information~~BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify~~recognize~~ BCSI~~BES Cyber System Information~~; or • Storage locations identified for housing BCSI~~BES Cyber System Information~~ in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicability**	**Requirements**	**Measures**
1.2	BCSI~~BES Cyber System Information~~ as identified in ~~Requirement R1~~ Part 1.1	Method(s) to protect and securely handle BCSI.~~prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BES Cyber System Information during storage, transit, use, and disposal.~~	Examples of acceptable evidence include, but are not limited to, the following: • Evidence of methods used to protect and securely handle BCSI during its lifecycle, including:~~prevent the unauthorized access to BES Cyber System Information (e.g., encryption of BES Cyber System Information and key management program, retention in the Physical Security Perimeter).~~ o Electronic mechanisms, o Physical mechanisms, o Technical mechanisms, or o Administrative mechanisms • ~~BES Cyber System Information~~BCSI is handled in a manner consistent with the entity's documented procedure(s)~~and key management program, retention in the Physical Security Perimeter)~~.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.3	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Process(es) to authorize access to BES Cyber System Information based on need, as determined by the Responsible Entity, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of the process to authorize access to BES Cyber System Information and documentation of when CIP Exceptional Circumstances were invoked. • This may include reviewing the Responsible Entity's key management process(es).

CIP-011-3 Table R1 – Information Protection Program			
Part	Applicability	Requirement	Measure

1.~~4~~3	BCSI~~BES Cyber System Information~~ as identified in ~~Requirement R1~~ Part 1.1~~.~~	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk identification and assessment method(s) for the following:~~Process(es) to identify, assess, and mitigate risks in cases where vendors store Responsible Entity's BES Cyber System Information.~~ 1.3.1 Data governance and rights management; and ~~Perform initial risk assessments of vendors that store the Responsible Entity's BES Cyber System Information~~ 1.3.2 Identity and access management; and ~~At least once every 15 calendar months, perform risk assessments of vendors that store the Responsible Entity's BES Cyber System Information~~ 1.3.3 Security management; and ~~Document the results of the risk assessments performed according to Parts 1.4.1 and 1.4.2 and the action plan to remediate or mitigate risk(s) identified in the assessment, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.~~	Examples of acceptable evidence may include, but are not limited to, dated documentation ~~of all~~ of the following: • Implementation of the risk identification and assessment method(s) (1.3);~~Methodology(ies) used to perform risk assessments~~ • ~~Dated documentation of initial vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity;~~ • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4);~~Dated documentation of vendor risk assessments pertaining to BES Cyber System Information that are performed by the Responsible Entity every 15 calendar months;~~ • Business agreements that include communication expectations and protocols for

		1.3.4 Application, infrastructure, and network security.	disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1);~~Dated documentation of results from the vendor risk assessments that are performed by the Responsible Entity; and~~ • Consideration made for data sovereignty, if any (1.3.1);~~Dated documentation of action plans and statuses of remediation and/or mitigation action items~~ • Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3); • Dated documentation of vendor's identity and access management program (1.3.2); and • Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).

1.4	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	Examples of evidence may include, but are not limited to, dated documentation of the following: • Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]); • Evidence of implementation (e.g., configuration files, command output, architecture documents); and • Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.5	BES Cyber System Information as identified in Requirement R1 Part 1.1.	For termination actions, revoke the individual's current access to BES Cyber System Information, unless already revoked according to CIP-004-7 Requirement R5, Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, documentation of the following: • Dated workflow or sign-off form verifying access removal associated with the termination action; and • Logs or other demonstration showing such persons no longer have access.

CIP-011-3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.6	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Verify at least once every 15 calendar months that access to BES Cyber System Information is correct and consists of personnel that the Responsible Entity determine are necessary for performing assigned work functions.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R1. Each Responsible Entity shall implement one or more documented key management program that collectively include the applicable requirement parts in CIP-011-3 Table R2 – Information Protection. *[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-011-3 Table R2 – Information Protection and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – Key Management Program			
Part	**Applicability**	**Requirement**	**Measure**
2.1	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Where applicable, develop a key management process(es) to restrict access with revocation ability, which shall include the following: 2.1.1 Key generation 2.1.3 Key distribution 2.1.4 Key storage 2.1.5 Key protection 2.1.6 Key periods 2.1.7 Key suppression 2.1.8 Key revocation 2.1.9 Key disposal	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s), including key generation, key distribution, key storage, key protection, key periods, key suppression, key revocation and key disposal are implemented; and • Configuration files, command output, or architecture documents.

CIP-011-3 Table R2 — Key Management Program			
Part	Applicability	Requirement	Measure
2.2	BES Cyber System Information as identified in Requirement R1 Part 1.1.	Implement controls to separate the BES Cyber System Information custodial entity's duties independently from the key management program duties established in Part 2.1.	Examples of evidence may include, but are not limited to, the following: • Dated documentation of key management method(s) that illustrate the Responsible Entity's independence from its vendor (e.g., locations where keys were generated, dated key period records for keys, access records to key storage locations). • Procedural controls should be designed to enforce the concept of separation of duties between the custodial entity and the key owner.

R2~~3~~. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2~~3~~. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R~~3~~2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~3~~2.1	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	Prior to the release for reuse ~~or disposal~~ of applicable ~~BES~~ Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media ~~shall be sanitized or destroyed~~.	Examples of acceptable evidence include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI. ~~• Records that indicate the Cyber Asset's data storage media was sanitized or destroyed before reuse or disposal.~~ ~~• Records that indicate chain of custody was implemented.~~

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI~~BES Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~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.~~

~~1.3.~~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 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~~ applicable ~~E~~entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority~~CEA~~ to retain specific evidence for a longer period of time as part of an investigation:

- ~~Each~~ The ~~Responsible~~ applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If an ~~Responsible~~ applicable ~~E~~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 Compliance Enforcement Authority~~CEA~~ shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. **Compliance Monitoring and Assessment Processes:** 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~

- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)	~~N/A~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)	~~The Responsible Entity has documented or implemented a BES Cyber System Information protection program, but did not prevent unauthorized access to BES Cyber System Information by eliminating the ability to obtain and use BCSI during storage, transit, use and disposal. (1.2)~~ The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)	The Responsible Entity ~~has~~ did not ~~documented or~~ implement~~ed~~ one or more ~~a~~ documented ~~BES Cyber System~~ information protection program(s). (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
~~R2~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A When the Responsible Entity used a vendor's services for BCSI as identified in Requirement R1, Part 1.1, the Responsible Entity documented one or more electronic technical mechanisms to prevent unauthorized logical access to BCSI but did not implement electronic technical mechanisms to prevent unauthorized logical access to BCSI. (R2)~~	~~When the Responsible Entity used a vendor's services for BCSI as identified in Requirement R1, Part 1.1, Tthe Responsible Entity has did not documented or implemented electronic technical mechanisms to prevent unauthorized logical access processes forto BCSI key management program. (R2)~~
R~~3~~2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI~~BES~~	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI~~BES~~	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber System Information~~ from the BES Cyber Asset. (2~~3~~.1)	~~Cyber System Information~~ from the BES Cyber Asset. (2~~3~~.~~1~~2)	Asset Reuse and Disposal. (~~R3~~R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their ~~BES Cyber System Information~~BCSI.

~~*Note: The Guidelines and Technical Basis section has not been revised as part of Project 2019-02. A separate technical rationale document has been created to cover Project 2019-02 revisions. Future edits to this section will be conducted through the Technical Rationale for Reliability Standards Project and the Standards Drafting Process.*~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Address the increased scope of the CIP-011 "Applicability" column now present in the updated Requirement R1 and new Requirement R2, which is focused on protection of BCSI. ;
- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Develop a risk management method(s) to evaluate vendors' environments for data governance and rights management; identity and access management; security management (physical and cyber); and application, infrastructure, and network security; and
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011.

The 18-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide ERO and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- ~~Interchange Coordinator or Interchange Authority~~
- Reliability Coordinator
- Transmission Operator
- Transmission Owner
- Facilities[2]

Background

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2~~, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3~~.

[1] See subject standards for additional information on Distribution Providers subject to the standards.
[2] See subject standards for additional information on Facilities subject to the standards.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

General Considerations

This standard will become effective 18 months following regulatory approval. The 18-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Address the increased scope of the CIP-011 "Applicability" column now present in the updated Requirement R1 and new Requirement R2, which is focused on protection of BCSI. ~~Establish and/or modify vendor relationships to establish compliance with the revised CIP-011-3 Requirements~~;
- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services~~Address the increased scope of the CIP-011-3 "Applicable Systems" and "Applicability" column, which has a focus on BES Cyber System Information as well as the addition of Protected Cyber Assets (PCA)~~; ~~and~~

~~Develop additional sanitization programs for the life cycle of BES Cyber Systems, if necessary;~~

- Develop a risk management method(s) to evaluate vendors' environments for data governance and rights management; identity and access management; security management (physical and cyber); and application, infrastructure, and network security; and
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011.

The 18-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide ERO and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection
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 eighteen (18) 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 eighteen (18) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

CIP-004-~~7~~ 6 – Cyber Security - Personnel & Training
Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-~~3~~ 2 – Cyber Security - Information Protection
Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-02 BES Cyber System Information Access Management** by **8 p.m. Eastern, September 21, 2020.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

Background Information

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Questions

1. Do you agree the revisions to CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions (e.g., cloud services)?

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree the revisions to CIP-004 clarify that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI?

   ☐ Yes
   ☐ No

   Comments:

3. Do you agree the revisions to CIP-011 clarify the protections expected when utilizing third-party solutions (e.g., cloud services)?

   ☐ Yes
   ☐ No

   Comments:

4. Do you agree the new and revised VSL/VRF descriptions clearly align with the revisions to CIP-004 and CIP-011?

   ☐ Yes
   ☐ No

   Comments:

5. The SDT is proposing an 18-month implementation plan. Do you agree to the proposed timeframe?

   ☐ Yes
   ☐ No

   Comments:

6. The SDT proposes that the modifications in CIP-004 and CIP-011 meet the project scope in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

7. Provide any additional comments for the standard drafting team to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-7

August 2020

RELIABILITY | RESILIENCE | SECURITY




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

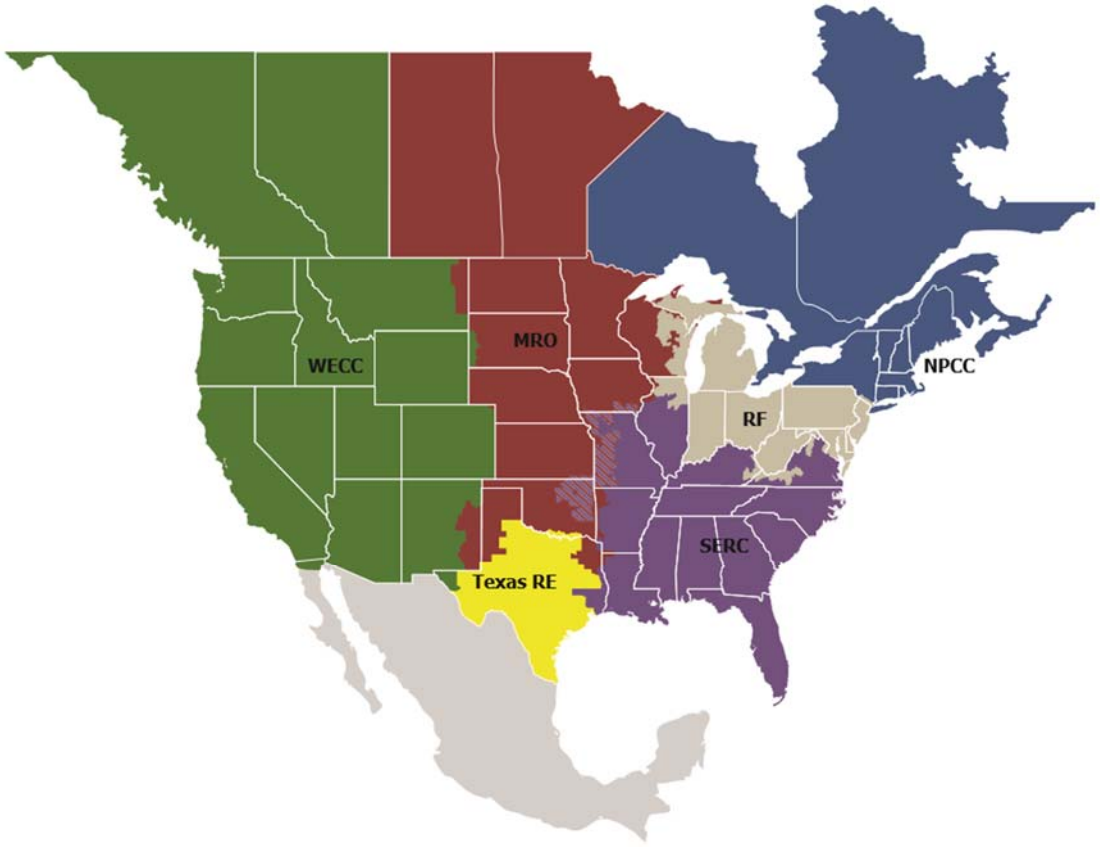
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the intent of the Standard Drafting Team (SDT) in drafting the requirements. This Technical Rationale and Justification for CIP-004-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving and initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-004-7 to require Responsible Entities to implement specific controls in Requirement R6 for provisioning, periodic review, and revocation of access related to BES Cyber System Information.

New and Modified Terms Used on NERC Reliability Standards

Proposed Modified Terms

None

Proposed New Terms

None

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1

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

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

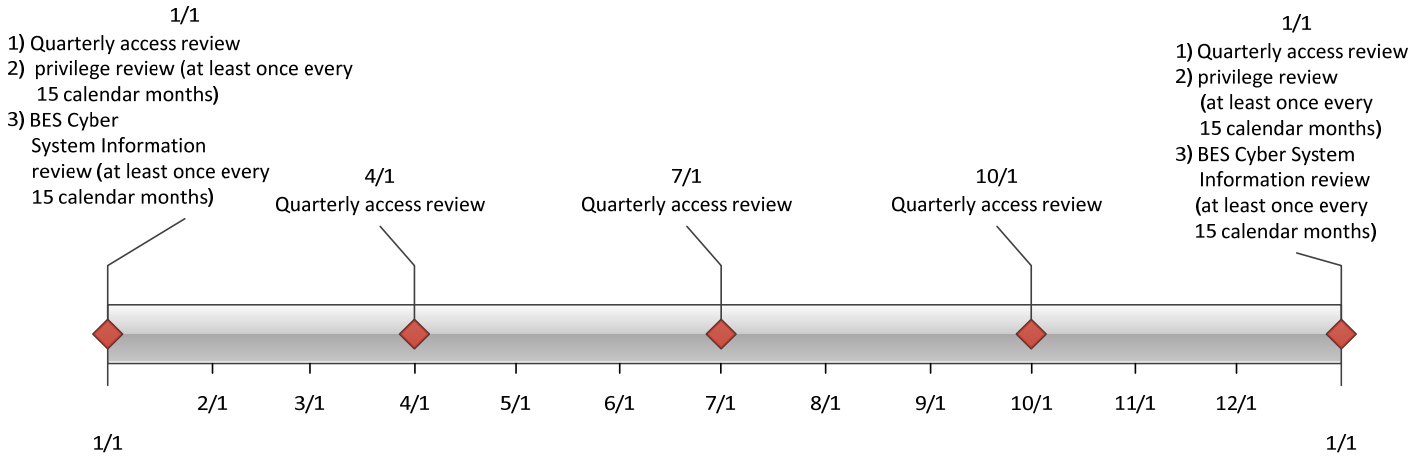
Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, the SDT intends that access authorization and provisioning be performed by different people where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

An example timeline of all the reviews in Requirement R4 is included below.



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

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

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

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

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

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information access management program with specific controls for access authorization, periodic review of provisioned access, and access revocation related to BES Cyber System Information, which, if accidentally or maliciously misused, could negatively impact the reliable operation of the Bulk Electric System. Authorization ensures only individuals who have a need are authorized for provisioned access to BES Cyber System Information. The periodic review ensures access is still required and has been provisioned appropriately and accurately. Revocation of access when individuals are terminated helps prevent inappropriate disclosure of sensitive information.

Requirement R6 shifts the focus to authorizing provisioned access to BES Cyber System Information itself. This is important when considering vendor services in which BES Cyber System Information is outside of the Responsible Entity's direct control.

Methods to document and track authorization for access where provisioning of access is a prerequisite of being able to obtain and/or use the BES Cyber System Information.

The SDT intends that access requirements do not apply to BES Cyber System Information where no specific provisioning mechanisms are available or feasible, or where provisioning is not specific to provisioning access to BES Cyber System Information. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room. There will likely be no specific provisioning of access to BES Cyber System Information on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BES Cyber System Information is only temporarily or incidentally located or stored there. The previous concept of designated storage locations was meant to exclude these locations. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BES Cyber System Information that may be located there. In these cases, access authorization, periodic review of provisioned access, and access revocation related to BES Cyber System Information would not be required. However, BES Cyber System Information in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required in CIP-011-3.

The SDT clarified the intent of addressing BES Cyber System Information as opposed to the BES Cyber System with associated applicable systems, which may contain BES Cyber System Information; the Applicability column has added language to specify BES Cyber System Information that is affiliated with associated applicable systems. In addition, the title of the column has been changed to "Applicability" to accommodate this philosophical change.

Requirement 6.1 has been drafted to ensure access authorization occurs only for individuals who have a need for provisioned access to BES Cyber System Information. Authorization should be considered to be a

grant of permission by a person or persons empowered by the Responsible Entity to perform such grants. Authorization for provisioned access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys). For BES Cyber System Information in physical format, physical access is provisioned to a physical storage location. For BES Cyber System Information in electronic format, electronic access is provisioned to an electronic system's front-end interface regardless of the geographical or physical location of the server or storage device or to individual encrypted files. Provisioning physical access to a physical location or storage device that contains electronic BES Cyber System Information is not considered provisioning access to electronic BES Cyber System Information. However, the Responsible Entity's information protection program and relevant information protection controls should be considered to prevent unauthorized access to BES Cyber System Information as required in CIP-011-3.

The SDT also intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R4, Part 4.1). Authorization for access to BES Cyber System Information must still be based on necessity of the individual performing a work function. Documentation showing the authorization should still have some justification of the business need included. To ensure proper segregation of duties, the SDT intends that access authorization and provisioning be performed by different people where possible.

Requirement 6.2 has been drafted to ensure the Responsible Entity reviews provisioned access privileges to BES Cyber System Information at least every 15 calendar months. The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges for BES Cyber System Information are the minimum necessary to perform their work function.

The SDT intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R4, Part 4.4). The 15-calendar-month review of BES Cyber System Information privilege is still in place to ensure an individual's associated privileges to BES Cyber System Information are the minimum necessary to perform their work function (i.e., least privilege). This involves determining the specific roles with BES Cyber System Information (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access to BES Cyber System Information does not assume any specific software, and it can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the BES Cyber System Information privilege review on individual accounts.

Requirement 6.3 ensures an individual who is involved in a termination action has their access to BES Cyber System Information promptly revoked. Access revocation (also referred to as "deprovisioning of access") is still understood to mean a process with the result that electronic access to BES Cyber System Information is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Access can only be revoked where access has been provisioned. Revoking access prevents any further access from that point in time onwards. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Responsible Entities should still consider the ramifications of deleting an account might include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The SDT intends for backwards compatibility with the previous requirement (CIP-004-6, Requirement R5, Part 5.3). The requirement to revoke access to BES Cyber System Information at the time of the termination action still includes procedures showing revocation of access to BES Cyber System Information concurrent with the termination action. This requirement also still recognizes the timing of the termination action might vary depending on the circumstance.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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:

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

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks

associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

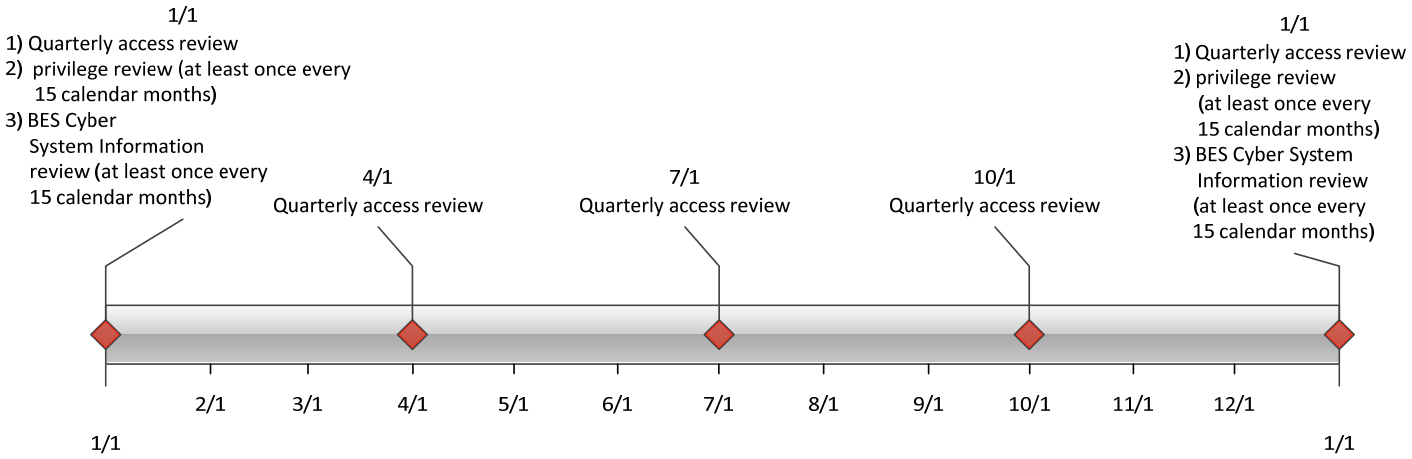
Requirement R4:

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

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

An example timeline of all the reviews in Requirement R4 is included below.



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

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

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

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

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

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this

requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

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

Rationale for Requirement R5:

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

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-3

August 2020

RELIABILITY | RESILIENCE | SECURITY




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

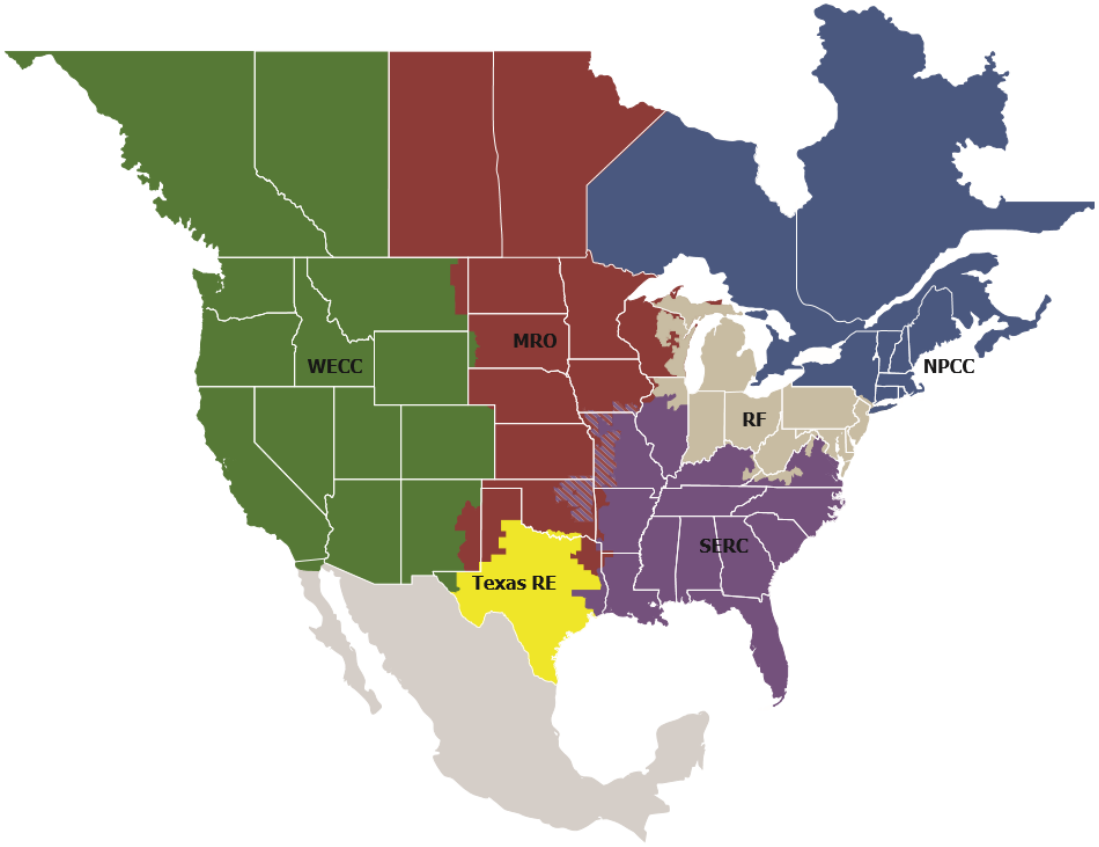
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-011-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving an initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI), by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-011-3 to require Responsible Entities to implement specific controls in Requirement R1 and Requirement R2 for procedural and technical controls related to BCSI during storage, handling, use, and disposal when implementing vendor provided services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

New and Modified Terms Used on NERC Reliability Standards

Proposed Modified Terms:

None

Proposed New Terms:

None

Rationale for Applicability Section

Standard CIP-011 has been modified to enhance protection of BCSI. The modified requirements under CIP-011 address protection of information in several facets that are discussed in this document, which include the following:

- Modifying the "Applicable Systems" column to "Applicability" where appropriate to specifically include BCSI
- Implement methods to identify risks involving vendor services related to BCSI
- Implement technical mechanisms to protect BCSI when engaging vendor services

To provide clarity, the Applicability Systems column, which now contains BCSI, is included to associate the requirement and address the focus on protecting the BCSI regardless of the location of the BCSI. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1:

Requirement R1 specifies procedural and technical controls for BCSI handling during storage, transit, use, and disposal including implementation of vendor-provided services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Requirement R1, Part 1.1, is intended to identify BCSI and provide documented methods to support this identification process.

The SDT clarified the intent of addressing BCSI as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicable Systems column includes language to specify BCSI "…pertaining to" the applicable systems. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, addresses methods to protect BCSI. Different states of information from the requirement; such as "transit" or "storage" are removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Rationale for New Requirement R1, Part 1.3

Requirement R1, Part 1.3, addresses the need for the Responsible Entity to understand details of the vendor's service environment and the vendor's controls where the entity's BCSI would be stored. This requirement contains technical detail specifically on the protection of BCSI. This is inherently different than CIP-013's overall risk approach to applicable systems and vendor-contracted relationships. This requirement is for implementing risk identification and assessment methods for the following sub requirements:

- Data governance and rights management
- Identity and access management
- Security management
- Application, infrastructure, and network security

Implemented identification and assessment methods are needed to understand the risks to BCSI when choosing to engage vendor services. It is important that the Responsible Entity conducts such due diligence to understand the risks related to the vendor's environment and controls given the compromise of BCSI involves critical infrastructure and recovery from compromise may be difficult due to the duration of remediation and related remediation costs. This is different than many other industries that are capable of superseding compromised information in a relatively short period of time. There are risks that cannot be mitigated directly in the vendor environment due to the lack of Responsible Entity control. This requirement ensures that, prior to BCSI entering a vendor's environment, the

Responsible Entity is well informed regarding the vendor's environment and controls and influences what, if any, varying controls offered by a vendor are utilized, or may influence the Responsible Entity's use of technical mechanisms (see CIP-011, R1.4) for which the Responsible Entity has more control.

The intent of addressing BCSI is clarified as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI; the Applicable Systems column includes language to specify BCSI that is pertinent with associated applicable systems. In addition, the title of the column is "Applicability" to accommodate this philosophical change.

The SDT's intent of the information protection program is to protect BCSI.

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BCSI be identified. The Responsible Entity has flexibility in determining how to implement the requirement.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Part 1.2 requires one or more methods for the protection and secure handling of BCSI. This includes information that may be stored on Transient Cyber Assets or Removable Media.

It is not the intent of this standard to mandate the use of one particular format for secure handling during transit of BCSI.

Rationale for New Requirement R1, Part 1.4:

The SDT's intent of the information protection program is to protect BCSI.

Requirement R1, Part 1.4, specifies technical, logical controls for the protection of electronic BES Cyber System Information during storage, transit, use, and disposal when implementing vendor-provided services such as SaaS, IaaS, or PaaS.

Requirement R1, Part 1.4, requires Responsible Entities to implement technical mechanisms to protect BCSI when engaging vendor services. Technical mechanisms provide a layer of defense against compromise needed to ensure a vendor's staff might have the means to electronically obtain BCSI but not use or modify BCSI. Technical mechanisms to protect BCSI are needed regardless of the location or state in which the Responsible Entity's BCSI resides when using vendor services. This requirement compliments R1, Part 1.3. Once, the risks are identified, appropriate technical mechanisms can be used to protect BCSI.

The intent of addressing BCSI is clarified as opposed to the BES Cyber System with associated applicable systems, which may contain BCSI. The Applicability column accommodates this philosophical change and to be consistent with the Applicability language added in Requirement R1, Parts 1.2 through 1.4.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 3 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

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 of Trustees approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-7, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-7, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5

The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-7, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified. .
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards**

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
Guideline 3- Consistency among Reliability Standards	This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) for BES Cyber System Information that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-7, R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented one or more documented access management program(s) for BES Cyber System Information (BCSI) but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items for Parts 6.1 through 6.3. (R6)	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

VSL Justifications for CIP-004-7, R6	
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	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby 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 VSLs are based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-3, Requirement R1

Requirement R1 was revised to eliminate potential compliance barriers for Responsible Entities that want to engage vendor services to store, utilize, or analyze BES Cyber System Information. The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

Requirement R1 was revised to include two new Parts (1.3 and 1.4) to eliminate potential compliance barriers for Responsible Entities that want to engage vendor services to store, utilize, or analyze BES Cyber System Information. Because there are now four Parts, the VSL was updated to include lower, moderate, and high VSL descriptions, which is more appropriate in case a violation moves beyond the control of the Responsible Entity (e.g., compromise of BES Cyber System Information while engaging vendor services). The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VRF Justification for CIP-011-3, Requirement R2

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R2

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 to CIP-004-7 R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R4, Part 4.1.3 Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	CIP-004-7, Requirement R6, Part 6.1 Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes a shift from authorization to access to designated storage locations, to authorizing the provisioning of BCSI access.
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information,	CIP-004-7, Requirement R6, Part 6.2, 6.2.1, and 6.2.2. Verify at least once every 15 calendar months that all provisioned access to BCSI:	Requirement R6 was created to house all BCSI related access management requirements, which include the current

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	6.2.1 Is authorized; and 6.2.2 Is appropriate based on need, as determined by the Responsible Entity.	CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is appropriate based on need.
CIP-004-6, Requirement R4, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	CIP-004-7, Requirement R6, Part 6.3 For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-2

The modifications made to requirements within CIP-011-2 are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use). In addition, new requirements have been implemented to mitigate risks associated with BCSI access when utilized in off-premises vendor services.

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	CIP-011-3, Requirement R1, Part 1.1 Method(s) to identify BCSI.	Requirement language simplified.
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	CIP-011-3, Requirement R1, Part 1.2 Method(s) to protect and securely handle BCSI.	Requirement revised to a focus around the implementation of controls that prevent the unauthorized access to BCSI (concurrent ability to obtain and use) in storage, transit, and use.
N/A	CIP-011-3, Requirement R1, Part 1.3 (NEW) When the Responsible Entity engages vendor services to store, utilize, or analyze	This new CIP-011-3 requirement is similar to the cyber security risk assessment required as part of CIP-013 Requirement R1, however it is intended to focus the risk assessment

Standard: CIP-011-3		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	BCSI, implement risk management method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	on the security controls used by the vendor to manage the environment that will be used to host Responsible Entity's BCSI.
N/A	CIP-011-3, Requirement Part 1.4 (NEW) When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.	This new CIP-011-3 requirement is intended to address any risks identified under CIP-011-3, Requirement R1, Part 1.3 through the implementation of technical controls to prevent unauthorized logical access to BCSI.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through September 21, 2020

Now Available

A 45-day formal comment period for **Project 2019-02 BES Cyber System Information Access Management** is open through **8 p.m. Eastern, Monday, September 21, 2020** for the following Standards and Implementation Plan:

CIP-004-7 - Cyber Security - Personnel & Training
CIP-011-3 - Cyber Security - Information Protection
Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Linda Jenkins regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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

Additional ballots for the standards and implementation plan, along with non-binding polls for each associated Violation Risk Factors and Violation Severity Levels will be conducted **September 11–21, 2020**.

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

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2019-02 BES Cyber System Information Access Management" in the Description Box. For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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:	2019-02 BES Cyber System Information Access Management (Draft 2)
Comment Period Start Date:	8/6/2020
Comment Period End Date:	9/21/2020
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 AB 2 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 2 ST 2019-02 BES Cyber System Information Access Management Implementation Plan AB 2 OT

There were 68 sets of responses, including comments from approximately 175 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree the revisions to CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions (e.g., cloud services)?

2. Do you agree the revisions to CIP-004 clarify that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI?

3. Do you agree the revisions to CIP-011 clarify the protections expected when utilizing third-party solutions (e.g., cloud services)?

4. Do you agree the new and revised VSL/VRF descriptions clearly align with the revisions to CIP-004 and CIP-011?

5. The SDT is proposing an 18-month implementation plan. Do you agree to the proposed timeframe?

6. The SDT proposes that the modifications in CIP-004 and CIP-011 meet the project scope in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

7. Provide any additional comments for the standard 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
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	Bobbi Welch	MISO	2	RF
					Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					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	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	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
Douglas Webb	Douglas Webb		MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6			Bob Solomon	Hoosier Energy Rural Electric	1	SERC

			MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations		Cooperative, Inc.		
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Frank Owens	Rayburn Country Electric Cooperative, Inc.	3	Texas RE
					Jim Davis	East Kentucky Power Cooperative	1,3	SERC
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Lincoln Electric System	Kayleigh Wilkerson	5		Lincoln Electric System	Kayleigh Wilkerson	Lincoln Electric System	5	MRO
					Eric Ruskamp	Lincoln Electric System	6	MRO
					Jason Fortik	Lincoln Electric System	3	MRO
					Danny Pudenz	Lincoln Electric System	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF

					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Northern California Power Agency	Marty Hostler	5		NCPA	Michael Whitney	Northern California Power Agency	3	WECC
					Scott Tomashefsky	Northern California Power Agency	4	WECC
					Dennis Sismaet	Northern California Power Agency	6	WECC
					Marty	Northern California Power Agen	5	WECC
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company -	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company -	1	SERC

Southern Company Services, Inc.						Southern Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC

Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
Brian Robinson	Utility Services	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Jim Grant	NYISO	2	NPCC

					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
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
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC

					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Do you agree the revisions to CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions (e.g., cloud services)?

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree with all of the revisions.

The measures for R6.2 are too detailed when referring to privileges. Many types of access to BCSI are binary, either you have it or you do not. Recommend the SDT remove the 3rd and 4th bullets in the measure so that an entity could simply verify that the access is still necessary and appropriate for their job.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The SDT should consider either defining the term “provisioned access” or removing it altogether in CIP-004 R6. The use of an undefined term such as “provisioned access” may lead to misunderstanding of the Standard and therefore may lead to inconsistent audit results. If you take “provisioned access” to mean only intentionally created individual accounts then administrative access to BCSI will not be governed by any Standard.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The addition of requirement 6 for CIP-004 makes it extremely difficult for entities to control access to BCSI. This is because of the requirement to provision access to individual pieces of information rather than provisioning access to where information is being stored (Storage locations).

We do not see how the changes clarify any requirements related to third-party solutions such as cloud services. Was the thought of changing the Applicability wording from "BCSI associated with" to "BCSI pertaining to" would provide the clarity that is being referenced? It is not obvious where any clarity is provided.

Likes 2	American Public Power Association, 4, Cashin Jack; Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

It is unclear in which instances provisioned access is applicable. Suggest include examples to clarify applicability by scenario (i.e.: cloud services).

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

For R6.1, the wording "based on need" is not necessary. SRP is not aware of any other reason that access would be authorized or than the fact there is a need for it. When access is authorized the fact there is a need is implied in the authorization. If it stays, how will you audit what is a valid "need"? If SRP authorizes access to everyone in a particular organization because SRP needs to comply with this requirement, is compliance a valid need? The focus should be on unauthorized access not appropriate business need.

For R6.1, the statement, "except for CIP Exceptional Circumstances" is not necessary. It's not clear if the exclusion "except for CIP Exceptional Circumstances" is stating in an Exceptional Circumstance it is not necessary to have business need or if it is not necessary to have authorization. (need to clarify) Even in an Exceptional Circumstance someone should still authorize the access – even though it might not follow the normal processes, at some level there is authorization, even if verbal.

For R6.1, in Measures, the statement "Dated authorization records for provisioned access to BCSI based on need". The statement based on need is not necessary here. If it is, then be clear on the expectations that the evidence needs to document the business need.

For R6.2, the wording “based on need” is not necessary. SRP supports requiring that the access “is authorized and appropriate as determined by the Responsible Entity.”

For R6.2, in Measures, if the requirement is to “Verify access to BCSI is appropriate based on needs” then why are the Measures silent on business need. Either remove business need or provide clarity on what is expected.

For R6.2, in Measures, the concept of “privileges” is not in CIP-004 R6, so it’s not clear how privileges will show compliance with the requirement. The Technical Rationale document states “Requirement 6.2 has been drafted to ensure the Responsible Entity reviews provisioned access **privileges** to BES Cyber System Information at least every 15 calendar months.” SRP does not see that in the R6.2 requirements.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

The change from BCSI storage locations to personnel with provisioned access to BCSI creates a significant administrative overhead for entities and is not practical resulting in no security value. The BCSI repository is the key for controlling access to BCSI and it is impossible to authorize and provision access to each single piece of BCSI. CIP-011 should require all BCSI must be stored within a repository in the first place. When a BCSI is taken outside BCSI repository for use, this should fall within CIP-011 on how to protect and handle BCSI. The current CIP-004 R4 and R5 has addressed the third-party storage issue as long as the third party is willing to provide evidence for compliance with CIP-004 R5 and R4. Resulting from lack of alternative controls for meeting CIP-004 requirements, the goal of the SAR is to create increased choices for utilization of modern third-party data storage and analysis systems. but the change from BCSI storage locations to provisioned access doesn’t resolve the issues and causes more confusion. We suggest the following wording for CIP-004 R6.1 based on the example 3 of SAR:

Process to authorize based on need, as determined by the Responsible Entity, except for CIP

Exceptional Circumstances:

6.1.1. Physical access to physical BCSI Repository;

6.1.2. Physical access to unencrypted electronic BCSI Repository;

6.1.3. Electronic access to unencrypted electronic BCSI Repository; and

6.1.4. Electronic access to BCSI encryption keys for encrypted BES Cyber System Information.

The above wording The Part 6.14 can fit cloud storage services well. We suggest defining the BCSI Repository term and requiring BCSI Repository identification in CIP-011.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
Puget Sound Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
The intent of this standard development project was to enable entities to utilize third party service providers for storage and analysis of BCSI by defining the security control requirements should entities choose to utilize third party services. Utilizing third party providers may result in increased reliability, increased choice, greater flexibility, higher availability, and reduced-cost for entities. Current CIP standards essentially do not address this scenario.	

The SDT introduced a requirement to develop and implement an access management program for BCSI brought forward as a new requirement (a new R6 and previous R4.1.3, R4.4 and R5.3 are moved to the new R6) in the proposed CIP-004-7. Controls introduced as part of this program are similar to that of access management for electronic and unescorted physical access to BES Cyber Systems.

The addition of Requirement R6 in the proposed CIP-004-7 (draft 2) has introduced additional access management controls applicable to all scenarios including those who manage their BCSI without utilizing third party. We believe requiring additional security controls outside of the context of utilizing a third party is out of scope of this project.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PAC does not agree with the revisions. The proposed revisions does not clarify the protections expected when utilizing third- party solutions (e.g., cloud services). The wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

PacifiCorp appreciates the change to the applicability to be consistent with the current version of the requirement.

We do believe this still allows for provisioned access to designated BCSI storage locations.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The applicable portion of the control is R6.1, which BPA believes is very broad and lacking specificity in its wording: “Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.” The SDT must continue to consider the

physical storage of printed materials as well, so as not to exclude the possibility of protecting physical storage locations under some facsimile of the current methodology.

Proposed change:

Authorize provisioning of access to BCSI as follows:

R6.1.1 Authorize physical access to physical BCSI based on need, except for CIP Exceptional Circumstances; and

R6.1.2 Authorize electronic access to electronic BCSI (including BCSI maintained by, stored at, or shared with a vendor for purposes of analysis) based on need, except for CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

1. There are very clear distinctions and limitations on the concept of what 'provisioned access' to BCSI constitutes and what it does not within the associated CIP-004-7 Technical Rationale document as drafted by the Standard Drafting Team. However, as this is not part of the CIP-004-7 standard itself, there is no guarantee that the Technical Rationale document guidance will be used as part of the compliance monitoring/enforcement approach, as regional enforcement agencies typically audit to the language of the standard. BC Hydro recommends that this clarity be incorporated directly into the CIP-004-7 standard requirements language to alleviate the risk of unintended interpretations in practice.
2. Require clarity as to whether CIP-004-7 Requirement 6 only applies to BCSI to which the Responsible Entity has the ability to directly control the provisioning of access and not to third-party service provider created or controlled repositories of BCSI (i.e. cloud services). For example, does this requirement apply to system administrators or support staff employed by a cloud service provider, or only to personnel with provisioned access to BCSI who are employed (either directly as employees/contractors or indirectly as sub-contractors) and who are terminated by the Responsible Entity?
3. Pending the answer to b), per CIP-004-7 Requirement 6.3, does the termination concept also apply to the cloud service provider's staff (or any other third-party service provider agency's staff members for that matter) and/or any of their sub-contractors who may be supporting a cloud service containing BCSI or managing a repository outside of the Responsible Entity's control?
4. The language of CIP-004-7 Requirement 6.2 only talks to the verification every 15 calendar months of provisioned access to BCSI (for authorizations and that access is appropriate based on need). The Measures however discuss the collection of evidence regarding specific privileges associated with authorizations and to compare against specific privileges that are provisioned as well. The concept of privilege reviews (i.e. least privilege) is also backed by the CIP-004-7 Technical Rationale document. This requirement needs further clarity to confirm whether 15-calendar month verifications are actually required to examine specific access privileges in addition to authorizations based on need or whether verifications of authorizations based on need is sufficient. If this is expected, should clarity that 'access privileges are appropriate based on need' be added to the standard requirement language.

Likes 0	

Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

The change from authorizing designated storage location access to “provisioned access to BCSI” does not clarify the requirements, especially since “provisioned access” is not a defined term. While the term has changed from designated storage locations to “provisioned access,” the meaning seems to be the same when you review information in the technical rationale. The change in the term creates significant administrative work to update program documentation, as well as access tracking tools, without commensurate improvement or flexibility in security controls.

In addition, the wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

MidAmerican Energy Company appreciates the change to the applicability to be consistent with the current version of the requirement.

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

The change from authorizing designated storage location access to “provisioned access to BCSI” does not clarify the requirements, especially since “provisioned access” is not a defined term. While the term has changed from designated storage locations to “provisioned access,” the meaning seems to be the same when you review information in the technical rationale. The change in the term creates significant administrative work to update program documentation, as well as access tracking tools, without commensurate improvement or flexibility in security controls.

In addition, the wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

MidAmerican Energy Company appreciates the change to the applicability to be consistent with the current version of the requirement.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) feels that Requirement R6 and its subparts do not provide clarity that one intent of these requirements is to manage access when utilizing third-party solutions since it doesn't explicitly make that statement. The phrase "provisioning of access" does not necessarily imply "when utilizing third party solutions." It is also ambiguous enough that it creates the impression that the phrase needs to be defined.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E believes the modifications are a good step in clearly indicting that access to BCSI must be defined for the BSCI and not storage locations as indicated under the current Standards. These changes would make use of third party service providers (i.e. vendor or cloud) possible, but the language of Requirement Part 6.1 is confusion. Is an Entity authorizing provisioning of access or provisioning authorized access. The Technical Rational (TR) document has the following for R6:

"Methods to document and track authorization for access where provisioning of access is a prerequisite of being able to obtain and/or use the BES Cyber System Information"

The above is clearer than the Requirement language in P6.1, but the TR is not the Standard and should not be counted on when audit teams start their interruption of the Standard. PG&E recommends the language for Part 6.1 be modified to more clearly indicate in the intent, such as:

"Provisioning of authorized access to physical and electronic BCSI based on need as determine by the Responsible Entity, except for CIP Exceptional Circumstances."

PG&E also indicates physical and electronic should be indicated in P6.2 and P6.3

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST notes the proposed revisions say nothing at all about third-party solutions, cloud-based or otherwise.

Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
Oklahoma Gas & Electric supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We support NPCC comments: We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
We do not agree that the revisions in CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions. There is no mention of utilization of third-party solutions such as cloud services or vendor services in the requirements and or technical rationale in regards to question 1 above: https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_Technical_Rationale.pdf https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_redline_to_last_posted.pdf Further, the requirements in CIP-011 use the term “vendor services”, which does not match the way question 1 is framed. The new technical rationale assumes BCSI is outside of the Responsible Entity’s direct control, but with electronic mechanisms implemented to protect BCSI via CIP-011 R1.4, BCSI would in fact be in the Responsible Entity’s direct control. The new technical rationale goes on to explain: “For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room.” Simply being able to view BCSI in a meeting, on a screen, etc., does not constitute access. To access something in which access is controlled, such as under a CIP-011 Information Protection Program, requires credentials with provisioned privileges, such as a key, username/password, encryption key, badge, fingerprint, etc. and provisioned permissions to gain access. The new technical rationale is confusing provisioning with credentials: “Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).” A process to grant access, contains the element of provisioning which is part of the considerations of need to know/access. When an access request is processed, physical access as an example, an individual isn’t given access to every PSP unless requested. If access to all PSPs were requested, the request would be reviewed for need, and approved or denied based on need. If approved, the individual would be provisioned with those access rights and credentials given to access the PSPs. The process of granting of access is the full complement of, request, assessing need, approval, provisioning, and credentials. Access revocation can be achieved by the removal of ALL provisioned access rights or disabling of credentials. Access can be reduced or increased by provisioning of rights. In CIP-004-6’s Guidelines and Technical Basis, page 44 states: “Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.”

The converse of revocation of access would be granting of access. The process of granting of access would result in providing individual(s) credentials with provisioned access privileges to access a BES Cyber System. Therefore we do not agree with the use of "provisioned access".	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not agree with the revisions to CIP-004. While public power supports that the revisions do not limit third party solutions, we also believe that the revisions are unclear about the requirement's applicability when using third-party solutions. APPA utilities want to be able to use third party solutions without unecessary regulatory risk.	
Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Comments: GSOC greatly appreciates the SDT's consideration of its previous comments regarding the consolidation of all access management related requirements into CIP-004. However, it does not support the revisions to CIP-004 to clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions – as proposed – and provides the following comments for the SDT's consideration: 1. **Modification of Established Format -** As stated in its previous comments, while GSOC understands what the SDT was attempting to accomplish, it does not agree with the replacement of "Applicable Systems" with "Applicability." "Applicability" is already utilized in each of the reliability standards to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope of applicability within body of CIP-004 will result in confusion and ambiguity regarding the overall applicability of this reliability standard. Further, this change results in this Standard and CIP-011 (where this change has also been proposed) being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. GSOC raises, for the SDT's consideration, that the deviation from the established format and scoping mechanisms used throughout the CIP reliability standard will create confusion and ambiguity and that any value achieved by this change will be far outweighed by the continued value associated with the current format and terms. To address this concern, GSOC proposes that the lead in requirement language for requirement R6 be modified as follows: Each Responsible Entity shall implement one or more documented access management program(s) for BES Cyber System Information ***about the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information*** that collectively include each	

of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].

2. **Potential Scope Expansion -** GSOC notes that it is also concerned that the modifications to the contents of the "Applicability" column may potentially expand and obscure the established definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. Specifically, the revisions limit the "applicability" to "BCSI associated with …" BCSI is defined as

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

The use of the term "associated with" is subjective and could be interpreted broadly by some entities and/or regulators. As an example, information about an external firewall configuration that acts as a first line of defense, but is not part of an applicable system, may contain information that "could be used to gain unauthorized access or pose a security threat to the BES Cyber System." It is unclear under the proposed revisions to the applicability column whether this information would be considered subject to CIP-004 – even if the asset from which it came is not in scope for any other reliability standards. This potential scope expansion and the associated ambiguity between the scope of CIP-004, the remaining reliability standards, and the Glossary of Terms Used in NERC Reliability Standards could result in increased compliance obligations without an attendant security or reliability benefit, confusion, and inconsistency of implementation. The proposed revision above would resolve this issue while preserving the current format of CIP-004 and its consistency with the remaining reliability standards.

3. Less flexibility/More restrictive language - As GSOC understands the draft, the objective of developing a dedicated requirement for access authorization to BCSI was to add flexibility for entities utilizing hosted services for BCSI storage, use, transit, etc. GSOC appreciates this objective and respectfully questions why the SDT utilized significantly different language in this requirement than the current "boilerplate" language utilized in the existing access authorization requirements – especially considering that the new language appears to be more restrictive. As an example, the current access authorization requirement language reads as follows:

Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter; …

The new language in requirement R6.1 reads as follows:

Authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances.

In requirement R6, the flexibility afforded to entities to define and implement an access authorization process (which may or may not specifically address provisioning depending on an entity's process and needs) has been removed and, although the technical rationale alludes to the ability to have no authorization or provisioning where such is not possible, the requirement, on its face, as proposed, does not appear to afford such flexibility.

Indeed, a plain reading of the requirement would indicate that access to any individual piece of BCSI would require authorized, provisioned access. For this reason, GSOC would respectfully suggest that this modification is unnecessarily restrictive and that the retention of the current boilerplate language (with minor revision) would afford Responsible Entities more flexibility to define their processes for both self-hosted and third-party hosted data within their BCSI program. For these reasons, GSOC recommends that the SDT revise the lead-in requirement language as indicated above and revise the proposed language for Requirement R6.1 to

Process to authorize access based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances

Finally, the value of driving consistency in rigor and format for access authorization must be considered. GSOC does not foresee that the value of changing the established format, applicability, and access-related obligations for one piece of the overall security framework that comprises the CIP reliability standards will outweigh the value of developing enhancements that conform with the established, known format, applicability, and access-related obligations currently in place.

4. Maintain consistency with established language – For the same reasons described above, GSOC would respectfully recommend that requirements R6.2 and R6.3 also be reverted to language similar to that currently utilized within the existing access management requirements, e.g.:

R6.2 Verify at least once every 15 calendar months that access to **BCSI or its designated storage location,** whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

R6.3 For termination actions, revoke the individual's access to **BCSI or its designated storage location,** whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.

5. Backwards compatibility - GSOC appreciates the SDT's consideration of the important concept of backwards compatibility in the Technical Rationale; however, the shift from access authorization by repository/location or BCSI to BCSI only appears to remove the ability of Responsible Entities to manage such authorizations, verifications, and terminations based on the use of designated storage locations or repositories. Many current programs have been developed and are managed around the concept of repositories or storage locations – not individual pieces of BCSI. For this reason, GSOC cannot agree that the proposed requirements are actually backwards compatible nor that minimal effort will be required to meet these new requirements. In particular, the proposed requirements focus solely on each individual piece of information and the management of access thereto. The obvious implementation method to ensure compliance would be to create and maintain a list of each individual piece of BCSI, its location, and its format. Such a list would be a new development that would likely not be compatible with existing program implementations.

6. Technical Rationale as support for revisions - GSOC notes the Technical Rationale does not appear to be consistent with the proposed revisions and does not make a convincing case for the significant changes proposed, e.g., revision of the requirement structure, inability to manage BCSI by location or repository, etc. To address this, GSOC proposes the above revisions, which would maintain the current format and provide flexibility for the management of BCSI via documented processes that can address either individual BCSI management, management by repository/location, or both. To ensure consistency between the Technical Rationale and the proposed revisions, GSOC respectfully suggests that the SDT review these documents objectively and make necessary revisions.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf, and in addition, submits the following comments below regarding CIP-004-7 Requirement 6, part 6.1.

Discussions with the Standard Drafting Team (SDT) have clarified that CIP-004-7 R6.1 was not intended to require provisioning of access to each individual piece of BCSI. The SDT explained that the language was written to accommodate a use case where the BCSI authorization attaches to the document so that the authorization follows the document when moved to various locations.

To accommodate both circumstances where entities may fall under the use case scenario or may use designated storage locations for BCSI, SDG&E proposes the following two options:

1. Provide two parts to the requirement. One part will be similar to the current CIP-004-6 R4.1.3 which requires authorization of access to BCSI designated storage locations. The other part will authorize the provisioning of access to BCSI for documents not stored in a designated storage location.

2. Given the possibly low frequency of the described use case, retain the current CIP-004-6 R4.1.3 BCSI designated storage location authorization requirement while adding a provision to ensure that documents not stored in BCSI storage locations are protected according to the other CIP information protection requirements.

Two other alternatives are suggested below:

Proposal No. 1:

Authorize provisioning of access to BCSI based on need **and** as determined by the Responsible **Entity's designated method(s) to protect and securely handle BCSI**, except for CIP Exceptional Circumstances.

Proposal No. 2:

Using one or a combination of the following methods, authorize provisioning of access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

- **Access to designated storage locations, whether physical or electronic, for BES Cyber System Information; or**
- **Access to BES Cyber System Information, whether physical or electronic.**

If the SDT does not adopt any changes to the CIP-004-7 R6.1 Requirement language, please consider adding clarifying language in the Measures and/or Technical Rationale explicitly stating that authorization of access to BCSI is not required for each individual piece of BCSI.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not agree with the revisions. The proposed revisions does not clarify the protections expected when utilizing third-party solutions (e.g., cloud services). The wording of requirement 6.2 expands the scope of the 15-month review by making it similar to the 4.2 quarterly requirement – verify that provisioned access is authorized. The requirement should be the same as CIP-004-6 R4.4 – verify that accesses are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.

NV Energy appreciates the change to the applicability to be consistent with the current version of the requirement.

NVE also supports EEI's comments on providing clarity on the language associated with Requirement R6, Part 6.1, and aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase “Process to”, which would place the responsibility on the entity to define its process.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	No
Document Name	

Comment

The term "provisioning" is ambiguous and could lead to various interpretations of the requirements across the regions. More detailed clarification is needed of the term is to remain in the language. Concerns over 3rd party access control and what appears to be additional lists and documantation.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	2019-02_Unofficial_Comment_Form_IRC SRC_FINAL_09-21-20.docx
Comment	

There is a lack of clarity around the implications of the new term “provisioning.” Until the ISO/RTO Council Standards Review Committee (IRC SRC) better understand these implications and expectations, we are concerned.

It seems like the SDT has attempted to break the process of providing access to BCSI into two component parts: The authentication process, which we are assuming is a much broader list, coupled with the technical controls that are being referred to in the standard as “provisioning.” The mandate would be that no user should be “provisioned” access without (first) being authorized. At first glance this seems to raise the compliance burden without providing any real security value.

It’s not clear to us how these changes are looking to facilitate the storage of BCSI by third party providers or even how the audit requirements would be met in the use case of utilizing cloud based services for the processing or storage of BCSI.

Another concern that we have is how this would be applied to physical controls on physical (non-electronic) documents.

We request clarification as to how third party access would be managed.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize ***the following*** based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. ***Physical access to physical BES Cyber System Information storage locations;***

4.1.4. ***Physical access to unencrypted electronic BES Cyber System Information storage locations***;

4.1.5. ***Electronic access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.6. ***Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information***

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment
We do not understand all of the implications of the new term “provisioning.” Until we better understand these implications and expectations, we are concerned. Not sure how these changes address our concerns with the third party access Not sure how the addition of another list helps - - - appears to be more work. Especially for physical security Request clarification whether the third party access should be managed on an individual basis or on the team The intent of this standard development project was to enable entities to utilize third party service providers for storage and analysis of BCSI by defining the security control requirements should entities choose to utilize third party services. Utilizing third party providers may result in increased reliability, increased choice, greater flexibility, higher availability, and reduced-cost for entities. Current CIP standards essentially do not address this scenario. The SDT introduced a requirement to develop and implement an access management program for BCSI brought forward as a new requirement (a new R6 and previous R4.1.3, R4.4 and R5.3 are moved to the new R6) in the proposed CIP-004-7. Controls introduced as part of this program are similar to that of access management for electronic and unescorted physical access to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
Management of provisioned access to BCSI, when utilizing third-party solutions, needs to be clarified. Requirement R6, part 6.1 states that entities are required to “authorize provisioning of access to BCSI based on need.” This could be read to mean, among other things, that entities are required to authorize someone to provision access to BCSI, provision access to all BCSI (i.e. requiring a provisioning authorization for each piece of BCSI), or a variety of other interpretations. To resolve this issue, EEI suggests aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase “Process to”, which would place the responsibility on the entity to define its process. Additionally, EEI suggests adding the following “Measure” to Requirement 6, Part 6.1: • A documented process used to define provisioned access to BCSI.

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Provisioned access terminology should be removed. When access revocation is necessary the provisioned access, as well as the authorization for access shall be removed.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please incorporate the guidance from the “Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020” document into the CIP-004 and CIP-011 revisions.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment

CAISO is in support of the below IRC SRC comments:

There is a lack of clarity around the implications of the new term “provisioning.” Until the ISO/RTO Council Standards Review Committee (IRC SRC)[1] better understands these implications and expectations, we are concerned.

It seems like the SDT has attempted to break the process of providing access to BCSI into two component parts: The authentication process, which we are assuming is a much broader list, coupled with the technical controls that are being referred to in the standard as “provisioning.” The mandate would be that no user should be “provisioned” access without (first) being authorized. At first glance this seems to raise the compliance burden without providing any real security value.

It’s not clear to us how these changes are looking to facilitate the storage of BCSI by third party providers or even how the audit requirements would be met in the use case of utilizing cloud based services for the processing or storage of BCSI.

Another concern that we have is how this would be applied to physical controls on physical (non-electronic) documents.

We request clarification as to how third party access would be managed.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize the following based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. Physical access to physical BES Cyber System Information storage locations;

4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;

4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and

4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

We do not agree that the revisions in CIP-004 clarify the requirements for managing provisioned access to BCSI when utilizing third-party solutions. There is no mention of utilization of third-party solutions such as cloud services or vendor services in the requirements and or technical rationale in regards to question 1 above:
https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_Technical_Rationale.pdf

https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/2019-02_CIP-004-7_redline_to_last_posted.pdf

Further, the requirements in CIP-011 use the term “vendor services”, which does not match the way question 1 is framed.

The new technical rationale assumes BCSI is outside of the Responsible Entity’s direct control, but with electronic mechanisms implemented to protect BCSI via CIP-011 R1.4, BCSI would in fact be in the Responsible Entity’s direct control.

The new technical rationale goes on to explain:

“For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BES Cyber System Information, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room.”

Simply being able to view BCSI in a meeting, on a screen, etc., does not constitute access. To access something in which access is controlled, such as under a CIP-011 Information Protection Program, requires credentials with provisioned privileges, such as a key, username/password, encryption key, badge, fingerprint, etc. and provisioned permissions to gain access. The new technical rationale is confusing provisioning with credentials:

“Provisioning should be considered the specific actions taken to provide an individual the means to access BES Cyber System Information (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).”

A process to grant access, contains the element of provisioning which is part of the considerations of need to know/access. When an access request is processed, physical access as an example, an individual isn’t given access to every PSP unless requested. If access to all PSPs were requested, the request would be reviewed for need, and approved or denied based on need. If approved, the individual would be provisioned with those access rights and credentials given to access the PSPs. The process of granting of access is the full complement of, request, assessing need, approval, provisioning, and credentials. Access revocation can be achieved by the removal of ALL provisioned access rights or disabling of credentials. Access can be reduced or increased by provisioning of rights. In CIP-004-6’s Guidelines and Technical Basis, page 44 states:

“Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.”

The converse of revocation of access would be granting of access. The process of granting of access would result in providing individual(s) credentials with provisioned access privileges to access a BES Cyber System. Therefore we do not agree with the use of “provisioned access”.

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 does not agree the revisions to CIP-004 provide enough clarity. While the Technical Rationale provides additional clarity, the enforceable requirement of "Authorize provisioning of access to BCSI based on need" is a virtually unlimited statement and is not scoped to where the BCSI is stored. It does not exclude BCSI in use. Entities cannot prove the prevention of "unprovisioned" personnel "accessing" BCSI such as hardcopies, or in discussions in a meeting. The Technical Rationale explicity acknowledges this dilemma, but those concepts do not make it to the enforceable language. We can provision access to BCSI where it is stored and with the loss of that concept within the language of the requirement, clarity is also lost.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the Comment Form submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with EEI's comments to rephrase R6.1 to mirror 4.1, "Process to authorize access to BCSI based on need…" Also, the written requirement should be clear about the requirements for authorizing access to BCSI stored in the cloud. Is the expectation that encryption with key management be utilized? Is merely obtaining access lists of personnel from the vendor sufficient, when the requirement states to authorize "based on need, as determined by the Responsible Entity"? The concern is that if NERC is looking for encryption, will they find individual	

entities who do not utilize encryption for BCSI in the cloud to have insufficient security controls in place, even if they requirement is written so as not to prevent that scenario.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 1.

Likes 0	
Dislikes 0	

Response

Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	Yes
Document Name	

Comment

Oncor supports EEI's comment.

Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Although the revision facilitates using a third-party solution, FEU suggests the SDT consider using a third-party example in the Measures of the new R6 requirements.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports the change from “designated storage locations” to “provisioned access”. It is backwards compatible, scopes applicability, clarifies requirements when utilizing cloud services, and better defines what access entities are expected to control. MPC also appreciates the use of the qualifier “provisioned” in front of the broad term “access” in R6, and the time invested in the technical rationale document and how it informs industry on what this qualifier means and does not mean. The broad term “access”, when used without context, has led to significant misinterpretation and unintended consequences of what constitutes “access to BCSI” vs “visibility/sharing of BCSI”, which makes the term “provisioned” an important differentiator and a good improvement.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

ATC appreciates the SDT's removal of BCSI from CIP-004-6 Requirements R4 and R5, and the result to keep this apart from the realm of physical access to where electronic BCSI may be physically stored, which has been a point of contention and confusion. Creating the new requirement R6 accomplishes this separation and clarity making it possible for the controls to not only be commensurate with risk, but also to be commensurate with the format of the BCSI and the types of methods available to protect digital vs hardcopy.

ATC also appreciates the use of the qualifier "provisioned" in front of the broad ranging term "access" in R6, and the time invested in the TR and how it informs industry on what this qualifier means and doesn't mean. The broad term "access" when used without context has led to significant misinterpretation and unintended consequences of what constitutes "access to BCSI" vs "visibility/sharing of BCSI" and making the term "provisioned" an important differentiator, and a good improvement.

ATC further appreciates how this proposed qualifier "provisioned" **scopes CIP-004** to that which the entity can **control**; meaning that access which we (the entity) authorizes, we can control what access we (the entity) provisions (configures).

- We cannot control another person's cognition and retention; and should not have requirements that misconstrue "see/hear/store in brain" as "access" as opposed to that invoking "handling protections for a business need to share on a temporary basis by a person with authorized provisioned access".
- Additionally, this approach helps prevent overreach in CIP-004 for controls on the "unauthorized access" side; Here, risk mitigation is more relevant. CIP-004 is about the controls to address the expected by providing the right access to the people who need it when they need it, and not about the logging, alerting, monitoring, prevention, detection, deterrence, and response measures that belong somewhere else outside of CIP-004 to address the unexpected. Mitigating controls like those in **CIP-011** are the ones that **help prevent** the "unauthorized access" from happening; which is very different than the intent of **CIP-004** which is to **control** the authorization and provisioning aspect.

CIP-004 – control what is in our control and manage authorized provisioned access

authorized = the people we expect to have access based on need;

provisioned = the people who are actually configured for that access;

provisioned can be a subset of authorized; an entity is not in violation if the list of authorized people is greater than the list of provisioned people as long as all who are provisioned are also authorized

CIP-011 – mitigate risk for that which we cannot completely control; an unauthorized individual gaining unauthorized access. By adding "provisioned" as a qualifier to CIP-004 access we scope the evidence further than it is today while also starting to remove the ability for industry to get dinged under CIP-004 for the unintended types of "access" that are on the wrong side of BOOM.

Likes 0	
Dislikes 0	

Response

Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
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	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on authorized provisioning as it applies to repositories versus discrete pieces of BCSI. Duke Energy would also like to know the difference between Authorized and Authorized provisioniong.Duke Energy needs more clarification on authorized provisioning as it applies to repositories versus discrete pieces of BCSI. Duke Energy would also like to know the difference between Authorized and Authorized provisioniong.	

Likes 1	Wabash Valley Power Association, 3, Sosbe Susan
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Becky Webb - Exelon - 6
Answer	
Document Name	
Comment
Exelon has elected to align with EEI in response to this question.
Likes 0	
Dislikes 0	
Response

2. Do you agree the revisions to CIP-004 clarify that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI?

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 2.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy agrees with EEI's comments.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

We do not agree with the new language in R6's requirements, which does not distinguish between physical and/or electronic access to BCSI and could cause confusion. We also disagree with the use of "provisioning of." Part of the process of granting access is provisioning access such as read-only, read/write, etc. There is no need to change the verbiage used in CIP-004 for access, as it has been used in the standards for years and is clear. If adding "provisioning of" to access for BCSI it should be added to electronic access and physical access. Adding this would cause further confusion and ambiguity to the requirements.

Further, while not all measures are necessary to meet the requirement, the measures for R6.2 for entities trying to meet or exceed the requirement are administratively burdensome and duplicative with the clause "not limited to" in the evidence examples.

Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO is in support of the below IRC SRC comments:

There needs to be more clarification on what constitutes "provisioning."

Today, technical access controls are used as physical security provisioning. We are concerned as to how these requirements are intended to be applied to non-electronic BCSI.

The IRC SRC would request that the intent of "provisioning" be spelled out more explicitly in the Measures instead of the Technical Guidance - - - possibly in 6.1.

In lieu of additional work to define "provision," we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize the following based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. Physical access to physical BES Cyber System Information storage locations;

4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;

4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and

4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

Please incorporate the guidance from the “Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020” document into the CIP-004 and CIP-011 revisions.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Although the technical rationale provides clarity on this issue, the language contained in CIP-004-7 does not provide similar clarity. Given compliance is based on the plain language of the Reliability Standard, EEI suggests the following modifications to CIP-004-7to provide greater clarity:

Requirement R6

Part 6.1: Authorize provisioning of **physical access and/or electronic access** to BCSI **as appropriate and** based on need,….

Part 6.2: Verify at least once every 15 calendar months that provisioned access to **physical and/or electronic** BCSI **as appropriate**:

Part 6.3: For termination actions, remove the individual’s ability to use provisioned access to **physical and/or electronic** BCSI **as appropriate** (unless already revoked according to Part 5.1) by the ……

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management

Answer	No
Document Name	

Comment

There needs to be more clarification on what constitutes “provisioning.”

Today, technical access controls are used as physical security provisioning. We are concerned as to how these requirements are intended to be applied to non-electronic BCSI.

The IRC SRC would request that the intent of “provisioning” be spelled out more explicitly in the Measures instead of the Technical Guidance - - - possibly in 6.1.

In lieu of additional work to define “provision,” we request the SDT consider eliminating requirement R6 and focus its efforts on modifying the existing language in requirement 4.1 using the examples from page 4 of the SAR as a starting point and making as few changes as possible to achieve the objectives. This would simplify the solution and streamline entity costs associated with transition. For example:

R4.1 Process to authorize ***the following*** based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access;

4.1.2. Unescorted physical access into a Physical Security Perimeter;

4.1.3. ***Physical access to physical BES Cyber System Information storage locations;***

4.1.4. ***Physical access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.5. ***Electronic access to unencrypted electronic BES Cyber System Information storage locations;***

4.1.6. ***Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information***

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	No
Document Name	

Comment

Again, the term "provisioning" is troublesome and will create confusion and inconsistencies.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy is aware that clarity on this topic ("...**manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI")** is provided within the supplemental Technical Rationale document for this Project, but this clarification should be added to the language of the requirement. Entities are audited to the plain language of the Standard, and not the Technical Rationale for the justification of a Requirement, so the CIP-004-7 should explicitly state that provisioning of access is for **physical access to physical BCSI and electronic access to electronic BCSI.** This will remove any ambiguity. Example would be to include the term, "physical access and/or electronic access to...", preceding BCSI in Part 6.1, 6.2, and 6.3	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
See SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Comments: No. GSOC does not agree that the revisions to CIP-004 clarifies that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI. If this is intended to be connoted by the introduction of the term "provisioned," GSOC would respectfully suggest that the insertion of that term is not enough to communicate the above concept and that the SDT consider additional revisions to clarify their intent. Further, GSOC is concerned that, the guidance in the Technical Rationale notwithstanding, the term "provisioned" is undefined. Accordingly, both the term and its associated activities could be both implemented and interpreted differently by various Responsible and Regional Entities. Finally, GSOC is concerned that the concept indicated above and the guidance provided in the Technical Rationale could leave a potential security gap around the management of BCSI. For example, what obligation do Responsible Entities have related to BCSI that is typically stored and managed electronically, but may be printed out or otherwise displayed? Conversely, where BCSI is typically stored and managed physically, but is converted to an electronic format to facilitate vendor or other review, what would a Responsible Entity's obligation be to authorize access thereto? GSOC appreciates that the SDT is trying to create flexibility around access management, but is concerned that the resulting ambiguity could create issues from both a security and compliance perspective.	
Likes 0	
Dislikes 0	

Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

Public power does not agee that the CIP-004 revisions specifically separate the compliance between providing physical access to BES cyber system information and electronic access to BES cyber system information. The requirement language does not distinctly separate the treatment of physical versus electronic BES cyber system information. APPA recommends that language be added making this distinction between physical and electronic access clear.

APPA supports the suggested way the language could be revised provided by Tacoma Power in their 2019-02 comments:

"Authorize provisioning of physical access to physical BCSI and electronic access to electronic BCSI, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances."

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

We do not agree with the new language in R6's requirements, which does not distinguish between physical and/or electronic access to BCSI and could cause confusion. We also disagree with the use of "provisioning of." Part of the process of granting access is provisioning access such as read-only, read/write, etc. There is no need to change the verbiage used in CIP-004 for access, as it has been used in the standards for years and is clear. If adding "provisioning of" to access for BCSI it should be added to electronic access and physical access. Adding this would cause further confusion and ambiguity to the requirements.

Further, while not all measures are necessary to meet the requirement, the measures for R6.2 for entities trying to meet or exceed the requirement are administratively burdensome and duplicative with the clause "not limited to" in the evidence examples.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

We support NPCC comments:

Need to nail down “provisioning” in order to answer Yes or No

Today’s technical access is the physical security provisioning.

Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1

Removing the notion of access to designated storage locations, whether physical or electronic reduces any ambiguity it may have had with respect to the management of physical access where the BCSI resides on a electronic form.

Emphasis could be placed on the concept introduced in the ERO Enterprise CMEP Practice Guide published on April 26, 2019 where access to the BCSI is defined by the individual ability to obtain and use the BCSI.

Depending on the security measures in place (e.g. encryption with key management), it makes it explicit that an individual with physical access to a data center containing BCSI, but without the ability to use the BCSI (due to encryption) would not be within the scope of the requirement.

For exemple:

6.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

Ability to obtain and use BCSI, wheter physical or electronic.

6.2 Verify at least once every 15 calendar months that all individual’s with ability **to obtain and use** BCSI:

6.2.1. Is authorized; and

6.2.2. Is appropriate based on need, as determined by the Responsible Entity

6.3 For termination actions, remove the individual’s ability to **obtain and use** BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	

Oklahoma Gas & Electric supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes the proposed revisions neither adequately define nor clearly convey what it means to "provision access" to BCSI. If someone is handed a piece of paper, on which is printed information classified as BCSI, has that individual been "provisioned" with "physical access to physical BCSI"? Similarly, has an individual been "provisioned" for "electronic access to electronic BCSI" if an electronic copy of that same document is sent to him or her via email? N&ST is concerned, based on 10 years of experience with compliance monitoring and enforcement programs, that if CIP-004 doesn't clearly define what "provisioning" means, audit teams will develop their own definitions (use of plural is intentional). N&ST recommends maintaining CIP-004's well-understood requirement to manage access to "designated storage locations," which may be electronic (e.g., a file server) or physical (e.g., a lockable file cabinet).

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The plain language of the Standard does not align with the language in the technical rationale for Requirement 6. DOminion Energy recommends the Requirement language be aligned with thetechnical rationale as follows:

Requirement R6

Part 6.1: Authorize provisioning of **physical access and/or electronic access** to BCSI **as appropriate and** based on need,….

Part 6.2: Verify at least once every 15 calendar months that provisioned access to

physical and/or electronic BCSI **as appropriate**:

Part 6.3: For termination actions, remove the individual's ability to use provisioned

access to **physical and/or electronic** BCSI **as appropriate** (unless already revoked according to Part 5.1) by the ……	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
While this is implied in the language of the Requirement R6 “Parts”, the lack of such words as physical or electronic does not make it clear the Requirements are for both. PG&E believes this lack of explicit reference to physical or electronic is problematic and should be corrected by clearly indicating the provisioning of access should be for physical and electronic BCSI as PG&E indicated in the answer to Question 1.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
Answer	No
Document Name	
Comment	
See SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

The CIP-004 Requirement R6 requirement revisions do not provide the clarity that entities are only required to manage the provisioning of physical access to physical BCSI and electronic access to electronic BCSI. The following suggested modification would make it clear;

· Part 6.1: Authorize provisioning of physical access to physical BCSI and/or electronic access to electronic BCSI based on need, …

· Part 6.2: Verify at least once every 15 calendar months that provisioned access to physical and/or electronic BCSI: …

· Part 6.3: For termination actions, remove the individual's ability to use provisioned access to physical and/or electronic BCSI (unless already revoked according to Part 5.1) by the …

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

Comments: No, this is not clear with the limited wording "provisioning of access." While there is additional information in the technical rationale, the requirement text itself does not clarify this point.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

No, this is not clear with the limited wording "provisioning of access." While there is additional information in the technical rationale, the requirement text itself does not clarify this point.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

1. The CIP-004-7 Technical Rationale document do explain this concept however this is not clear from the standard language itself. BC Hydro recommends that the clarity provided per the Technical Rationale be incorporated into the actual standard language or be formally adopted as NERC endorsed implementation guidance to avoid misinterpretations as the enforcement agencies typically audit to the language of the reliability standards and not to these additional documents.
2. Within the CIP-004-7 Technical Rationale document, the SDT's intent around provisioning of electronic access to electronic BCSI is not clear. There is specific mention of the following:

"For BES Cyber System Information in electronic format, electronic access is provisioned to an electronic system's front-end interface regardless of the geographical or physical location of the server or storage device or to individual encrypted files. Provisioning physical access to a physical location or storage device that contains electronic BES Cyber System Information is not considered provisioning access to electronic BES Cyber System Information." Further explanation is required as to what is considered the front-end interface. For example consider a server hosting a SharePoint platform which in turn contains BCSI. What is/are considered the front-end interface(s) in this case? The server OS? The Sharepoint platform itself? This should be clarified within the language of the standard or incorporated into a NERC endorsed implementation guidance document instead of limited to a Technical Rationale document to avoid misinterpretations. Enforcement agencies typically audit to the language of the reliability standards and not to Technical Rationale documents.

Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
See BPA's comments to Question 1, above.	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	

Comment
If the intent was to make clarification about explicitly mentioning physical and electronic access, the SDT will need to make further revisions to clarify that. CIP-004-6 is currently only require managing physical access to BCSI. The need to manage electronic access is not explicitly stated but falls under the requirement to protect BCSI under CIP-011-2 Requirement R1 and as part of entities' Information Protection program.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment
Managing the provisioning of physical access to physical BCSI is misleading. For instance, if all unencrypted BCSI are stored on a sever, does the server need to have authorized physical access? Obviously, the answer is Yes. However, if using the provisioned access language, the BCSI server physical access control would be ignored. The provisioned access to BCSI is not clear. When the BCSI is taken outside BCSI Repository, it is not practical for CIP-004 to manage the access to each piece of BCSI outside the BCSI repository. If a BCSI is under the personal control of the user who has authorized access to BCSI, it should be treated as BCSI access controlled and

should be addressed in CIP-011requirement for protecting and handling BCSI rather than in CIP-004. Also “authorized provisioned access to BCSI” has a wrong logical order since provisioning should happen after the authorization, but the wording can be interpreted to have authorization after provisioning.

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 proposed language is too ambigious and obligates entities to protect BCSI in any form, even though beyond its control. Should BCSI be shared with NERC/FERC, the way CIP-004 reads in present state could be understood so as to require registered entities to extend their access management to be inclusive of a copy of that information held by NERC/FERC. And subsequent requirements in CIP-011 would require reviews of access rights associated with that copy.

The language should be re-scoped to focus on management of access to designated repositories, instead of the information itself.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

We do not see how the changes make any differentiation from Provisioning of physical access to BCSI and electronic access to BCSI. Was the thought that changing the Applicability wording from “BCSI associated with” to “BCSI pertaining to”, would provide the clarity that is being referenced? It is not clear where any clarity is provided.

Likes 1	Platte River Power Authority, 5, Archie Tyson

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The enforceable language in this version does not differentiate between physical and electronic access. If electronic BCSI is not stored or transmitted in a protected form, then physical access to electronic BCSI could permit the bypass of any electronic access controls.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
Part 6.3: We understand provisioned access to be a subset of access, and that access grants can be provisioned, inadvertent, or obtained in other ways. We think the intent of this Part is to remove all of the terminated individual's accesses to BCSI, not just provisioned access. The 'use' consideration is just perhaps misplaced within the sentence? Consider replacing "remove the individual's ability to use provisioned access to BCSI" with "remove the individual's ability to access and use BCSI".	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
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

Southern agrees this is an important distinction to make and the revision to CIP-004 clarifies this electronic/physical distinction with the deletion of R4.1.3. The revision does pose an issue as entities cannot prove the prevention of personnel seeing hardcopies (physical/printed) of network diagrams or other forms of BCSI. However, the Technical Rationale does explicity acknowledge that dilemma. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or views a whiteboard in a conference room. There will likely be no specific provisioning of access to BES Cyber System Information on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. That now deleted language was unclear at best if this distinction was even allowed. Removal of R4.1.3 has clarified that it is now possible to make this distinction. However, making this distinction is implied but never stated in R6.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

ATC appreciates the SDT's removal of BCSI from CIP-004-6 Requirements R4 and R5, and the result to keep this apart from the realm of physical access to where electronic BCSI may be physically stored, which has been a point of contention and confusion. Creating the new requirement R6 accomplishes this separation and clarity making it possible for the controls to not only be commensurate with risk, but also to be commensurate with the format of the BCSI and the types of methods available to protect digital vs hardcopy. This is very important in order to enable use of cloud-based solutions for CIP BCSI.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment
BCSI requirements seem cleaner to be consolidated into R6, however the revisions have minimal impact to the provisioning aspects of the requirements. It has always been AEP's understanding that AEP is responsible the provisioning of physical access to physical BCSI and electronic access to electronic BCSI.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	

Comment
The concept of provisioned access to BCSI clarifies this, since provisioned access to a room where a physical server is housed does not in itself give access to the electronic BCSI on that server.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
: PAC agrees with the revision. New language verifies provisioned access to BCSI is authorized and the provisioned access is appropriate based on need.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SRP agrees, but does not fully agree with the current wording.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
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	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 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	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Carl Pineault - Hydro-Qu?bec Production - 5
Answer
Document Name
Comment
We support NPCC Regional Standards Committee 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 NPCC Regional Standards Committee
Answer
Document Name
Comment
Need to nail down “provisioning” in order to answer Yes or No Today’s technical access is the physical security provisioning. Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1 Removing the notion of access to designated storage locations, whether physical or electronic reduces any ambiguity it may have had with respect to the management of physical access where the BCSI resides on a electronic form. Emphasis could be placed on the concept introduced in the ERO Enterprise CMEP Practice Guide published on April 26, 2019 where access to the BCSI is defined by the individual ability to obtain and use the BCSI. Depending on the security measures in place (e.g. encryption with key management), it makes it explicit that an individual with physical access to a data center containing BCSI, but without the ability to use the BCSI (due to encryption) would not be within the scope of the requirement.

For exemple:

6.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

Ability to obtain and use BCSI, wheter physical or electronic.

6.2 Verify at least once every 15 calendar months that all individual's with ability **to obtain and use** BCSI:

6.2.1. Is authorized; and

6.2.2. Is appropriate based on need, as determined by the Responsible Entity.

6.3 For termination actions, remove the individual's ability to **obtain and use** BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

If the intent was to make clarification about explicitly mentioning physical and electronic access, the SDT will need to make further revisions to clarify that.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

Need to nail down “provisioning” in order to answer Yes or No

Today’s technical access is the physical security provisioning. Prefer the intent of “provisioning” to be in the Measures instead of the Technical Guidance - - - possibly in Part 6.1	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on provisioning and managing as it applies to repositories versus discrete pieces of BCSI and electronic access to electronic BCSI.	
Likes 0	
Dislikes 0	
Response	

3. Do you agree the revisions to CIP-011 clarify the protections expected when utilizing third-party solutions (e.g., cloud services)?

Kjersti Drott - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State does not agree with the revisions.

We think 1.2 could cause audit approach confusion. In the measures would the expectation be we have identified data in a true data lifecycle methodology or just during use, transit, rest? We recommend the drafting team provide examples of what could be part of the data's lifecycle so it is clear what is intended (even though all states may not be applicable to every lifecycle).

As worded, a violation of R1.4 could also be considered a violation of R1.2. (double jeopardy) Instead, recommend combining R1.2 and R1.4 into one requirement. Additionally, recommend remove "for the separation of duties" from the measure as that could be interpreted in different ways and is not needed anyway to relay the intent.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

While the revisions add clarity for protections expected when utilizing third-party solutions such as cloud services for storage purposes, the "vendor services to utilize and analyze BCSI" lanuage presents a number of issues. R1.4 risk identification and assessment methods, as written, implies that this must be completed for all vendors that may have access to electronic of physical documentation containing BCSI. Vendors may only utilize information while onsite or may be authorized for access to BCSI for an engagement, but may never actually utilize or store this information. In these situations, the requirements to have to identiy and assess risks (R1.4) and then enforce at least one or more electonic technical controls (R1.5) are not value-added activities to the organization. To avoid scope creep, NERC may consider defining Vendor Services to define exactly what services are in scope.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No

Document Name	

Comment

Regarding usage of BCSI: We are unsure if the CIP-011-3 requirements that use the acronym “BCSI” are enforceable when the acronym is not included in the “BES Cyber System Information” NERC Glossary term. The acronym first appears in the purpose statement for CIP-011-3, but should the enforcement of the requirement depend on the purpose statement? Consider updating the "BES Cyber System Information" glossary term to include the new BCSI acronym as part of the CIP-011-3 draft. The acronym field for that glossary term is currently blank.

Part 1.3: The requirement in Part 1.3.1 doesn’t explicitly include data sovereignty, although the measures suggests that data sovereignty should be included. The omission of data sovereignty risk consideration in the requirement could represent an unaddressed risk for BCSI in a cloud service provider environment. Consider clarifying intent by aligning the language of the requirement with the language of the measure.

Part 1.3: We are unsure if risk management methods were intended for all vendor services related to BCSI, or just for the storage, utilize, or analyze cases. Consider changing “storage, utilize, or analyze, to “… including but not limited to storage, utilize, or analyze BCSI…” to ensure that all vendor services related to BCSI are covered.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

CIP-011-3 R1 Part 1.3 uses these terms without an accompanying definition: Data governance, rights management, identity management, access management, security management, application security, infrastructure security, and network security. Some examples are given in the Measures, but clear definitions, or referenced to documents that provide definitions, should be included.

Part 1.3 also groups different concepts into a single sub-part. Consider separating single sub-parts into definied and catergorized separate sub-parts. For example, 1.3.4 Application security; 1.3.5 Infrastructure security; and 1.3.6 Network security.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No

Document Name	

Comment

Having “Data Governance” listed under 1.3 risk management methods seems out of place and maybe duplicative. The measurement for 1.3.1 also seems to imply requirements that are not in the requirement column. The requirements seem broad and the measures are less clear and seem to add to the requirements. How does requirement 1.3.3 “Security management” differ from “Application, infrastructure and network security.” Should some of these requirements fall into CIP-013 when contracts are established for services?

Consider remove Data Governance from the requirement.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA does not believe that the CIP-011 Requirements R1.3 and R1.4 are needed. CIP-011 R1.3 is within scope of CIP-013 service procurement and should be addressed as part of that assessment. R1.4 protections mechanisms are covered in CIP-011 R1.2 and do not need to be duplicated in R1.4. R1.2 does not put limits on the scope of the mechanisms, and applies to the BCSI in all cases durings its lifecycle. We recommend adding the clause in the measures first bullet point, *Evidence of methods used to protect and securely handle BCSI during its lifecycle, by any authorized party or individual, including:*. We believe inclusion of this statement will clarify that the scope of the protection methods established are inclusive of the environments, transmission, and any interactions with the information.

Under Requirement 1.1 the changes to the standard moves the protection to the BCSI itself rather than the repositories that housing it. The last measure, which identifies storage locations, should be removed or modified to allow the entity to demonstrate the data flow of BCSI from the source BCS after identification. The language as proposed would make every BCA a BCSI storage location.

In requirements R2.1 and R2.2, the scope should be limited to Cyber Assets that contain accessible BCSI.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP agrees with the overall direction and what this version is trying to accomplish. We struggle with the four sub requirements in R1.3. We believe there is overlap and potential confusion in terms. For example, isn't "identity and access management" and "network security" a part of "security management"? The term "security management" is too broad. How is "rights management" different than "identity and access management"?

Also, when putting the R1.3 Requirement into individual sentences, they read:

- Implement risk management method(s) for **Data governance and rights management**
- Implement risk management method(s) for **Identity and access management**
- Implement risk management method(s) for **Security management**
- Implement risk management method(s) for **Application, infrastructure and network security**.

SRP suggests removing each of them from unique subrequirements.

Also, our concern is the wording provides too much flexibility in determining methods and defining the four topics. This will result in a wide range of methods implemented. We fear as written this requirement will create unintended consequences and become as difficult to interpret and implement as CIP-013 has been for the industry.

The technical rationale on the bottom of page 2 states "Implemented identification and assessment methods are needed to understand the risks to BCSI when choosing to use vendor services." This statement is more clear on what to do for R1.3 than what is written in the proposed requirement. Consider verbiage like this without subrequirements.

R1.3 and R1.4 read different than R1.1 and R1.2. R1.1 and R1.2 start with "Method" and R1.3 and R1.4 start with an applicability statement. The applicability statement should be in the applicability column.

Consider updating the Applicability in R1.3 and R1.4 to:

"**BCSI as identified in Part 1.1 when the Responsible Entity engages vendor services to store, utilize, or analyze BCSI**"

Then the R1.3 requirement can read:

"Implement one or more processes for identifying the risk of using vendor services to store, utilize, or analyze BCSI"

Then the R1.4 requirement can read:

"Implement one or more documented electronic technical mechanisms to protect BCSI when using vendor services to store, utilize, or analyze BCSI"

Overall, we need better clarification on how this is the same or different than CIP-013.

Likes 1	Platte River Power Authority, 5, Archie Tyson
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment
Part 1.3 should belong to CIP-013 since it is a vendor risk assessment item. Using requirement CIP-004 Part 6.1.4 we suggest in question 1, CIP-011 Part 1.4 should be moved to the Measures of CIP-004 Part 6.1.4 on how to control the access to the BCSI repository. CIP-011 requirements like other CIP-004 requirements should apply to the responsible entities as well as vendors by default and don't need to define vendor only requirements in CIP-11. The current version of CIP-011, vendor requirements are described in Guidelines and Technical Basis.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment
Recommend a change to Part 1.4's requirement to explicitly say "electronically." Change from When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. To When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	

Response

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo

Answer	No
Document Name	

Comment

The proposed R1.3 does not state any security controls that need to be implemented. The proposed R1.3 essentially requires entities to have a framework to manage risks associated with utilizing third party for storing, utilizing or analyzing. The proposed risk management framework needs to be implemented for 1.3.1 to 1.3.4.

We also believe that the term “utilize” in the proposed R1.3 is too broad. Requirements should focus on storage and analysis only.

While we welcome this approach since a one solution fits all may not exist; however, practicality of implementing such a framework is not clear. Perhaps, similar language to CIP-013 may be needed (risk-based approach) and use of terms such as the “the risk management methods need to address”.

The proposed R1.4 no longer suggests that protection at BCSI level (encryption) is a must. Instead, CIP-011 R1 will require a mechanism to protect BCSI. We still believe that protection must be applied at the BCSI level when stored/analyzed on a third party cloud.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided temporary access to a document that is considered BCSI. Clarification in the standard language or applicability should address the intended scope.

CIP-013 doesn’t require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties that are not Registered Entities compliance to the requirements.

Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
While the sub-parts of CIP-011-2 R1.3 appear to *imply* protections are only for electronic BCSI stored by vendor services. The language of the standard does not explicitly make this distinction. The language should be clarified accordingly to avoid confusion pertaining to physical BCSI for which vendor services may be engaged to store, utilize, or analyze BCSI.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
The SAR references “third party storage and analysis” but the requirement refers to “vendor services to store, utilize or analyze BCSI.” The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided a drawing that is considered BCSI. Change the text to be consistent with the SAR: “third party storage and analysis.” Consider limiting the scope to “data hosting” vendor services. If it was the standard drafting team’s intent to exclude temporary use of BCSI, it should be addressed in the technical rationale or requirement text. Also, there is nothing in the technical rationale excluding other entities and regulators from being considered “vendors.” CIP-013-1 R2 includes language that should be considered for CIP-011 R1.2: vendor performance and adherence to a contract are beyond the scope of the requirement. Remove the prescriptive sub parts on 1.3 and make the requirement simply: implement risk management methods. Allow the Registered Entities the flexibility to determine the appropriate components of risk management. Also, limit the requirements to match the applicability of CIP-004-6 R6. This should not be required for medium impact without ERC. To improve clarity, repeat the applicability on each subpart, rather than referring back to an earlier subpart.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

The SAR references “third party storage and analysis” but the requirement refers to “vendor services to store, utilize or analyze BCSI.” The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided a drawing that is considered BCSI.

Change the text to be consistent with the SAR: “third party storage and analysis.” Consider limiting the scope to “data hosting” vendor services. If it was the standard drafting team’s intent to exclude temporary use of BCSI, it should be addressed in the technical rationale or requirement text. Also, there is nothing in the technical rationale excluding other entities and regulators from being considered “vendors.”

CIP-013-1 R2 includes language that should be considered for CIP-011 R1.2: vendor performance and adherence to a contract are beyond the scope of the requirement.

Remove the prescriptive sub parts on 1.3 and make the requirement simply: implement risk management methods. Allow the Registered Entities the flexibility to determine the appropriate components of risk management.

Also, limit the requirements to match the applicability of CIP-004-6 R6. This should not be required for medium impact without ERC. To improve clarity, repeat the applicability on each subpart, rather than referring back to an earlier subpart.

Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CEHE agrees that the CIP-011 Requirement R1, Parts 1.3 and 1.4 clarify the protections expected when using third-party cloud services. However the requirement has much broader language that could be problematic. First, the term “Vendor services” goes beyond cloud services and could create unintended issues for other types of vendor services. Second, use of the term “BCSI” can imply both physical and electronic BCSI, which may cause a

problem because sub-part 1.3.4 would not apply to physical BCSI. Additionally, Part 1.4 that requires an entity to "implement documented electronic technical mechanisms" could not be applied to physical BCSI.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	No
Document Name	

Comment

See Tristate (SAR originator) and SMUDs comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E believes the modifications to clarify that third party solutions can be used, but the Requirement language in Parts 1.3 and 1.4 are vague. PG&E understands the vagueness is necessary to allow for the many possible methods of protecting BCSI with a third-party. PG&E believes the Measures and Technical Rational (TR) document provide sufficient information to allow an Entity to adequately protect their BCSI, but the Measures and TR are not the Standard which could lead to interpretation differences between an Entity and Audit Team. PG&E does not have a suggestion at this time to improve the vagueness but is willing to work with the SDT and industry to address this concern.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment
DOminion Energy supports the comments by EEI and agrees for the need to replace or clarify the term vendor services with a more narrowly and clearly defined term. There should be a clear deliniation between services that are off-premise and those that are housed on infrastructure directly controlled by the entity.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment
Regarding CIP-011-3 R1 Part 1.3, the terminology for the sub-parts do not add value to CIP-011. It is unclear what this terminology would require or what any of these terms mean, making them subject to broad and differing interpretation. The risk, which is unauthorized access, is currently being addressed by an entity's approach to satisfying CIP-011 part 1.2 and CIP-004 R6. What is the justification for this language if protection and access management is already required? The phrase "implement risk management" is unclear and open to interpretation. This proposed requirement is a paperwork exercise that adds administrative burden without realizing security benefits. Auditability will be difficult and open to interpretation. For these reasons, MPC proposes striking this requirement and relying on access management in CIP-004 and CIP-011 part 1.2 for protection of BCSI. For R1, parts 1.3 and 1.4, the phrase "engages vendor services to store, utilize, or analyze BCSI" does not clarify when or where this requirement is applicable. This could apply to an onsite vendor or contractor, when it seems this requirement is intended to address cloud service providers. MPC requests SDT consideration of alternative phrasing for 1.3, if CIP-011 part 1.3 is not struck as requested above, and 1.4 such as: "…service provider on service provider-owned or -managed premises or computing infrastructure…"

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3	
Answer	No
Document Name	

Comment
'Utilizing' leaves room for guessing. Why not consistently say – "transit, storage and use" like everywhere else in the document? AEP is also concerned with any unintended consequences from the proposed language, as it could be interepted to mean any vendor's use of BSCI, even if it is stored on AEP's systems, and not BSCI that is stored, transmited, or used by a 3rd party vendors on their system(s).

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes proposed Requirement R1 Part 1.3 has two significant problems. The first is that it seems to have been developed with vendor risk management in mind. If so, N&ST believes requirements to evaluate the risks associated with allowing any particular vendor to "store, utilize, or analyze" BCSI should be added to CIP-013, not CIP-011. The second is that in N&ST's opinion, the language of sub-parts 1.3.1 through 1.3.4, (e.g., 1.3.1, "Data governance and rights management") is vague to the point of lacking any intrinsic meaning. Furthermore, while we generally don't comment on proposed Measures, we are at a loss to understand what the example, "Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security control s as well as physical access controls" is intended to mean.

N&ST is also concerned about proposed Requirement R1 Part 1.4. While we agree it is a good security practice to "implement one or more documented electronic technical mechanisms to protect BCSI," we note the proposed requirement, as written, appears to apply only to situations where "the Responsible Entity engages vendor services to store, utilize, or analyze BCSI."

Finally N&ST notes that the latest revisions appear to have removed the requirement to protect BCSI (against, we presume, unauthorized disclosure), while "in transit." N&ST assumes this was unintentional.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

Oklahoma Gas & Electric supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

We support NPCC comments:

Recommend a change to Part 1.4's requirement to explicitly say "electronically."

Change from

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

To

When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

We agree that the revisions clarify the protections expected to be compliant, however, if it is the SDT's intent to have a risk assessment performed for 3rd party storage systems, then those requirements should be a part of CIP-013. This is not in the scope of the SAR, but should have been considered.

Secondly, requirements R1.3.1-1.3.4, are very dynamic for the majority of major Cloud Service Providers (CSP) and would require periodic/continuous risk assessments due to the nature of 3rd party storage services. As a 3rd party storage service customer, you are at the mercy of the CSP's terms and conditions, features, security features, IAM, encryption, etc. which may change at any time causing a change in risks. A change in terms and conditions, security features, IAM, purchasing additional security features, etc. would trigger a new risk assessment that would make compliance onerous.

Also, the configuration (hybrid, private, public) of cloud/3rd party services, severely impacts the potential threats to the unauthorized access to BCSI which is not considered in the requirements. For major CSPs as a 3rd party storage solution provider in a private configuration is no different than the BCSI being stored on premise.

Lastly, the way the question is being asked using “third-party solutions” (e.g. cloud services) instead of the language used in the requirements makes it difficult to answer without making assumptions.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC appreciates the use of the word “vendor” instead of “third party” to assure clarity that this refers to an entity that is not a Registered Entity. That having been said, the proposed words in CIP-011=3 might not go far enough on two points.

1. The words in CIP-011-3 Requirement R1 Parts 1.3 and 1.4 do not accomplish the level of specificity needed to assure the scope is appropriately limited to cloud type, off-premises solutions/services owned and managed by an entity that is **not** a Registered Entity. Unfortunately, the words as currently proposed carry the unintended consequence that a Registered Entity would have to perform a risk assessment on their own on-premises infrastructure. Additionally, to enable use of cloud-based solutions for BCSI while maintaining an objective, risk-based, and technology/platform agnostic requirement is equally important

2. In the current proposed draft, the use of the defined term BCSI without a scoping adjective of “electronic” or “digital” preceding it in these requirements continues to breed confusion that physical methods may also be needed; creating misalignment with the SAR’s intent is to enable use of electronic controls as the methods to protect BCSI where off-premises cloud-based solutions are used. The existing CMEP Practice Guide makes a concerted effort to separate physical controls for physical BCSI from electronic controls for electronic BSCI, bringing great clarity to the fact that electronic controls can be as secure, if not potentially more secure for electronic format BCSI than the physical controls like a PSP. This requirement language must achieve that same level of clarity to enable these requirements for cloud to actually be implemented without any misunderstanding that physical controls also must apply.

For these reasons, ATC requests SDT consideration alternative phrasing like this.

CIP-011-3 Requirement R1 Parts 1.3

1.3 For storage, utilization, or analysis of electronic BSCI performed by a service provider on service provider-owned or -managed premises or computing infrastructure, implement risk management method(s) for the following:

1.3.1 Data governance and rights management; and

1.3.2 Identity and access management; and

1.3.3 Security management; and

1.3.4 Application, infrastructure, and network security.

CIP-011-3 Requirement R1 Parts 1.4

1.4 For storage, utilization, or analysis of electronic BSCI performed by a service provider on service provider-owned or -managed premises or computing infrastructure, implement one or more documented electronic technical mechanisms to protect BCSI.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC greatly appreciates the SDT's consideration of its previous comments regarding the retention of all BCSI program requirements in CIP-011. However, it does not support the revisions to CIP-011 to clarify the protections expected when utilizing third-party solutions (e.g., cloud services) – as proposed – and provides the following comments for the SDT's consideration:

1. **Modification of Established Format** - As stated in its previous comments, while GSOC understands what the SDT was attempting to accomplish, it does not agree with the replacement of "Applicable Systems" with "Applicability." "Applicability" is already utilized in each of the reliability standards to denote whether or not a particular registered function has responsibility under the Standard. Utilization of the same term, but with a different scope of applicability within body of CIP-011 will result in confusion and ambiguity regarding the overall applicability of this reliability standard. Further, this change results in this Standard and CIP-004 (where this change has also been proposed) being different from the remaining CIP reliability standards relative to the CIP reliability standards overall approach to identification of asset scope. GSOC raises, for the SDT's consideration, that the deviation from the established format and scoping mechanisms used throughout the CIP reliability standard will create confusion and ambiguity and that any value achieved by this change will be far outweighed by the continued value associated with the current format and terms.

To address this concern, GSOC proposes that the lead in requirement language for requirement R6 be modified as follows:

Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information about the "Applicable Systems" identified in CIP-0011-3 Table R1 – Information Protection Program that collectively include each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

2. Potential Scope Expansion - GSOC notes that it is also concerned that the modifications to the contents of the "Applicability" column may potentially expand and obscure the established definition of BCSI set forth in the Glossary of Terms Used in NERC Reliability Standards. First, GSOC notes that the Applicability columns proposed between CIP-004 and CIP-011 are different. In particular, CIP-004 utilizes the terms "BCSI associated with …" while CIP-011 utilizes the terms "BCSI pertaining to…" BCSI is defined as

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES

Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

The use of the term "pertaining to…" is similarly subjective to the term "associated with" and could, therefore, also be interpreted broadly by some entities and/or regulators. As an example, information about an external firewall configuration that acts as a first line of defense, but is not part of an applicable system, may contain information that "could be used to gain unauthorized access or pose a security threat to the BES Cyber System." It is unclear under the proposed revisions to the applicability column whether this information would be considered subject to CIP-004 – even if the asset from which it came is not in scope for any other reliability standards. Moreover, these new terms as proposed in CIP-011 and CIP-004, although similar, could be interpreted differently between these two related standards, between Responsible Entities, and between Responsible Entities and Regulators. Such differing interpretations could result in both compliance and security-related concerns.

Finally, this potential scope expansion, conflict, and the associated ambiguity between the scope of CIP-004, CIP-011, the remaining reliability standards, and the Glossary of Terms Used in NERC Reliability Standards could result in increased compliance obligations without an attendant security or reliability benefit, confusion, and inconsistency of implementation. The proposed revision above would resolve this issue by eliminating the differing terms, while preserving the current format of CIP-011 and its consistency with the remaining reliability standards.

3. Backwards compatibility – GSOC is concerned that the proposed revisions for requirements R1.1 and R1.2 may not be compatible with Responsible Entities' existing programs. More specifically, many current programs have been developed and are managed around the concept of repositories or storage locations – not individual pieces of BCSI. The modifications of requirements R1.1and R1.2 (when coupled with the revisions to the Applicability Column) appear to shift focus to each individual piece of information – without flexibility to identify information based on their repository or storage location.

For this reason, GSOC respectfully suggests that the proposed requirements are not backwards compatible and would require significant effort to implement. This is because the obvious implementation method to ensure compliance would be to create and maintain a list of each individual piece of BCSI, its location, and its format. Such a list would be a new development that would likely not be compatible with existing program implementations. To address these concerns, GSOC recommends rewording requirement R1.1 as follows:

Method(s) to identify BCSI or their storage locations/repositories, as applicable

This would allow entities the flexibility to manage BCSI based on the most secure approach to such management, e.g., by repository or by pieces of information as it applies to their environment.

4. Ambiguity – GSOC is concerned that a number of the proposed revisions introduce ambiguity that could lead to differing interpretations and implementation for requirements R1.2 – R1.4. Relative to requirement R1.2, GSOC respectfully suggests that, contrary to the Technical Rationale, the removal of state references from the requirement and their replacement with more generic terms increases confusion and does not make the obligations more "explicitly comprehensive." In particular, GSOC notes that the previous state references (use, storage, transit, etc.) were well known and well understood concepts. Their replacement with a generic requirement to "protect and securely handle" could result in various interpretations and implementation of those obligations. Moreover, it could result in a security-related deficiency should an entity construe such terms narrowly.

Additionally, relative to requirements R1.3 and R1.4, GSOC is concerned that the term "vendor solutions" could be interpreted broadly to include "on-premises" vendor solutions that are managed by the responsible entity. For example, if an entity purchases and hosts "on prem" a document management system provided by a vendor, e.g., IBM, Microsoft, etc., would that "vendor solution" be subject to CIP-011, requirements R1.3 and R1.4. It is unclear from the language contained in the proposed revisions or the Technical Rationale what comprises or meets the definition of "vendor services." Accordingly, this term is open to interpretation and could lead to an overall scope expansion for this small subset of requirements – as unintended as that scope increase may be. Moreover, such scope expansion may increase Responsible Entity's obligations without an attendant increase in overall security or reliability – especially where additional requirements are applied to "on prem" "vendor solutions" that are managed by responsible Entities.

Further, GSOC notes that the terms introduced in requirement R1.4 may not all be well understood across the industry and should not be introduced without definitions or other guidance. As an example, the term "data governance" is not a well understood term across the industry and is not defined in these proposed revisions. Introducing this term and its associated "rights management" without any scope, context, or definition that would elucidate what it means in this use would be problematic as it has a high potential for confusion, ambiguity, and subjective interpretation. Moreover, as applied to potential "vendor solutions" (whether on- or off-premises), requirements R1.3 and R1.4 may be duplicative of each other and may be duplicative of what

is required in CIP-004 as well as other reliability standards. At a minimum, GSOC recommends combining requirements R1.3 and R1.4 and better defining those instances to which they apply.

5. Unintended consequences - GSOC is concerned that the proposed revisions to CIP-011 and CIP-004 result in significant program modifications and additional obligations for Responsible Entities regardless of whether they are using any cloud services, and, further, without modifications, vendors who have not engaged any cloud services and have not, therefore, modified their BCSI programs could be found non-compliant with these revised requirements. It respectfully asserts that requiring Responsible Entities that are not engaging in cloud-based services to overhaul their entire information program to support others who want to migrate to the cloud is manifestly unfair, unduly burdensome and a risk to reliability.

The placement of new and unnecessary compliance obligations and the potential expansion of the scope of CIP-011 for those entities that have chosen not to engage in the storage, handling, or use of BCSI in a cloud has the potential to divert resources to the implementation of new and different program aspects. Such diversion increases the risk of a deficiency or failure for issues that would be better addressed in implementation or compliance guidance. For these reasons, GSOC is concerned that the proposed revisions are not properly scoped to ensure compatibility with existing programs while accommodating the evolving storage and other solutions that could be employed in the future.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
See Tristate (SAR originator) and SMUDs comments.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The SAR is focused on cloud service providers, but the requirement potentially pulls in many other vendor services, such as engineering consultants who may occasionally be provided temporary access to a document that is considered BCSI. Clarification in the standard language or applicability should address the intended scope. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties that are not Registered Entities compliance to the requirements.	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
R1.4 should specify "electronically store".	
Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management

Answer	No
Document Name	

Comment

The IRC SRC recommends a change to Part 1.3's requirement as detailed below. Recommend any additional detail needed to describe risk management methods be captured under CIP-013.

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s).

Recommend a change to Part 1.4's requirement to explicitly say "electronically" as detiled below:

When the Responsible Entity engages vendor services to ***electronically*** store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Recommend a change to Part 1.4's requirement to explicitly say "electronically."

Change from

When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

To

When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.

Alternatively the Applicability column could specify "electronic."

The proposed R1.3 does not state any security controls that need to be implemented. The proposed R1.3 essentially requires entities to have a framework to manage risks associated with utilizing third party for storing, utilizing or analyzing. The proposed risk management framework needs to be implemented for 1.3.1 to 1.3.4.

We also believe that the term "utilize" in the proposed R1.3 is too broad. Requirements should focus on storage and analysis only.

While we welcome this approach since a one solution fits all may not exist; however, practicality of implementing such a framework is not clear. Perhaps, similar language to CIP-013 may be needed (risk-based approach) and use of terms such as the "the risk management methods need to address".

The proposed R1.4 no longer suggests that protection at BCSI level (encryption) is a must. Instead, CIP-011 R1 will require a mechanism to protect BCSI. We still believe that protection must be applied at the BCSI level when stored/analyzed on a third party cloud.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI recognizes SDT efforts to clarify the protection expectations needed by entities when utilizing third-party solutions but suggests the following changes to better clarify the needed protections:

Requirement 1

Part 1.2 Measures

1. EEI suggests modifying Bullet 2 to begin with the phrase "evidence demonstrating" to further clarify the Measure
2. EEI suggests adding the following measure: A documented process for protecting and securely handling BCSI.

Part 1.3 & 1.4: "Vendor services" is an overly broad term that is not limited to cloud services, and when combined it with the phrase "to utilize or analyze BCSI", brings in additional scenarios, such as engaging a vendor service on-premise at the Responsible Entity's location with the Responsible Entity's equipment to analyze BCSI (for example, in an incident response/forensics situation). Additionally, the requirement language does not link vendor services to BCSI that is stored, used, or analyzed off-premise on a vendor's infrastructure. "Engaging a vendor service" encompasses more than a cloud service offering and the resulting 1.3.1-1.3.4 methods are not applicable to a vendor providing services on site using the entity's own equipment. Both 1.3 and 1.4 begin with "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement …." We suggest changing both to clarify cloud-based scenarios such as "When the Responsible Entity engages ***off-premise*** vendor services to store, utilize, or analyze BCSI, implement…" or possibly "When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI ***on the vendor's infrastructure***, implement…"

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
While the revisions do clarify the protections expected when utilizing third-party solutions, the revisions do not have a narrowed scope. BCSI may be shared with mock auditors who will be analyzing BCSI. More clarity is required on the measures to determine the intended scope of the requirement changes. Unclear if these requirements are retroactive to contracted vendors or if these will apply to only new vendors.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please elaborate on what is required for CIP-011 R1.3.1 Data Governance and Rights Management.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	

Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	

Comment
CAISO is in support of the below IRC SRC comments: The IRC SRC recommends a change to Part 1.3's requirement as detailed below. Recommend any additional detail needed to describe risk management methods be captured under CIP-013. When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk management method(s). <To remove the below: "for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.">> Recommend a change to Part 1.4's requirement to explicitly say "electronically" as detiled below: When the Responsible Entity engages vendor services to electronically store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI. Alternatively the Applicability column could specify "electronic."

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	

Comment

We agree that the revisions clarify the protections expected to be compliant, however, if it is the SDT's intent to have a risk assessment performed for 3rd party storage systems, then those requirements should be a part of CIP-013. This is not in the scope of the SAR, but should have been considered.

Secondly, requirements R1.3.1-1.3.4, are very dynamic for the majority of major Cloud Service Providers (CSP) and would require periodic/continuous risk assessments due to the nature of 3rd party storage services. As a 3rd party storage service customer, you are at the mercy of the CSP's terms and conditions, features, security features, IAM, encryption, etc. which may change at any time causing a change in risks. A change in terms and conditions, security features, IAM, purchasing additional security features, etc. would trigger a new risk assessment that would make compliance onerous.

Also, the configuration (hybrid, private, public) of cloud/3rd party services, severely impacts the potential threats to the unauthorized access to BCSI which is not considered in the requirements. For major CSPs as a 3rd party storage solution provider in a private configuration is no different than the BCSI being stored on premise.

Lastly, the way the question is being asked using "third-party solutions" (e.g. cloud services) instead of the language used in the requirements makes it difficult to answer without making assumptions.

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 does not agree that CIP-011 clarifies the protections expected when utilizing third-party solutions. Per the TR, the different states of information from the requirement have been removed. "By removing this language, methods to protect BCSI becomes explicitly comprehensive." The SDT needs to clarify exactly what that means. Removing the language now seems to cause more confusion where this was intended to address.

The methods in requirement **R1.2** state to "protect" and "securely handle" BCSI. The two seem to be synonomous with each other and have no difference. Suggested restatement to simply use "securely handle" which has greater clarity and is sufficient on its own. The final bullet within the measures reads as a statement rather than an example of evidence as well as restates the information listed in the first bullet and should be changed to be an example of evidence different than the first bullet, or removed altogether.

R1.3 "Vendor services" is an overly broad term that is not limited to cloud services. When combined with "to utilize or analyze BCSI", it now includes numerous scenarios such as engaging a vendor service on-premise at the Responsible Entity's location with the Responsible Entity's equipment to analyze BCSI (example: a computer forensics company on retainer that is brought in to analyze an incident with a BCS). There is nothing in the requirement language that scopes it to BCSI that is stored, used, or analyzed off-premise on the vendor's infrastructure. "Engaging a vendor service" encompasses much more than a cloud service offering and the resulting 1.3.1-1.3.4 methods are not applicable to a vendor providing services on site using the entity's own equipment.

R1.3.3 (Security management) is a superset of the other three areas. 1.3.1 covers security of the data, 1.3.2 covers security of people, 1.3.4 covers security of the technology so 1.3.3 seems duplicative unless the intent is '*physical* security management' and if that is the intent, we suggest making that explicit.

The second bullet under Measures states that a list of risk assessment methods is "per vendor". We suggest striking this bullet as its covered by the first bullet and entities may have one risk management method that applies to all vendors, not per vendor.

R1.4 has the objective of simply "protect BCSI" but does not clarify "protect from what." The last bullet point under the Measure implies we are to protect the BCSI from subversion of the entity's control(s) by the custodial vendor. If that is the objective, we suggest that be placed in the requirement language for clarity as to the objective. Without further clarity, R1.4 is simply one scenario of R1.2.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Agree with EEI's comments regarding confusion around "vendor services." If the SDT's intent is not to include BCSI in transit or for vendor services not storing but utilizing and analyzing BCSI for a short term/temporary engagement, that should be made clearer.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar and Kansas City Power & Co, Evergy companies, incorporate by reference Edison Electric Institute's response to Question 3.

Likes 0	
Dislikes 0	

Response

Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	

Comment

The expectations regarding the utilization of third-party services seem clearer in this draft. However, with respect to CIP-011, specifically R1.4, it is apparent that a full security assessment will need to be performed on the vendor(s) in order to ensure compliance with the standard. As such, it would be helpful if the “Measures” section referenced specific acceptable standard certifications, such as SSAE 18 or FedRAMP. It should also be noted that vendors do not typically provide their security plan, when requested. This may make holistic security assessments difficult to complete.

Likes 0	

Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy needs more clarification on what constitutes “engaging in vendor services” versus need to know sharing of a limited piece of BCSI with a third-party consultant.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree the new and revised VSL/VRF descriptions clearly align with the revisions to CIP-004 and CIP-011?

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

We do not agree with the VSL/VRF because of our answer in question #3 above.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is in support of the below IRC SRC Comments:

Within CIP-004: Changes were with R4, R5 and new R6.

Within CIP-011: Request clarification that violating more than two of the sub-requirements (ex. Part 1.3), not the items beneath 1.3

Request clarification that violating more than two of the sub-requirements (ex. Part 1.3) counts as just Part 1.3 or a failure at the R1 level.

Earlier version of CIP-011 appeared to be more Pass/Fail. This version has gotten much more granular in its description and implementation in sub-requirements. The auditing has generally occurred at the highest level (ex. Level 1 not Level 1.1, 1.2, 1.3). With the greater detail in the sub-requirements, flexibility decreases and the administrative burden required to demonstrate compliance increases without commensurate security benefits. If a Responsible Entity failed on one of the (new) sub-requirements, the violation is still rolled out at the R1 level. In looking through the VSLs, the changes between Lower and Severe amplify in relation to the number of sub-requirements missed as opposed to how many times the overall requirement was missed.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment	
We support NPCC Regional Standards Committee 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 NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	
Comment	
Within CIP-004: Changes were with R4, R5 and new R6. Within CIP-011: Request clarification that violating more than two of the sub-requirements (ex. Part 1.3), not the items beneath 1.3 Request clarification that violating more than two of the sub-requirements (ex. Part 1.3) counts as just Part 1.3 or a failure at the R1 level. Earlier version of CIP-011 appeared to be more Pass/Fail. This version has gotten much more granular in its description and implementation in sub-requirements. The auditing has generally occurred at the highest level (ex. Level 1 not Level 1.1, 1.2, 1.3). With the greater detail in the sub-requirements, flexibility decreases and the administrative burden required to demonstrate compliance increases without commensurate security benefits. If a Responsible Entity failed on one of the (new) sub-requirements, the violation is still rolled out at the R1 level. In looking through the VSLs, the changes between Lower and Severe amplify in relation to the number of sub-requirements missed as opposed to how many times the overall requirement was missed.	

Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
Better clarification is needed as to which items fall into the violations versus the items below CIP-004 Part 6.2 and CIP-011 Part 1.3	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The proposed VSLs/VRFs align with the proposed revisions for CIP-004 and CIP-011.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
We do not agree with the VSL/VRF because of our answer in question #3 above.	
Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We support NPCC comments: Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST's response to this question is based on our objections to the proposed revisions to CIP-004 and CIP-011.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	No
Document Name	

Comment
AEP believes that with the possible extension of BCSI to cloud providers, and the fact that there have been significantly more sophisticated, and a greater volume of, attacks against the energy industry, especially through phishing, that the VRF for R1 should be High. Additionally, with known foreign ownership, control, or involvement in PC reclamation and recycling, and the focus of foreign adversaries trying to gain access, cause damage, or control the US Power grid, the VRF for R2 should also be High. We agree with the VSLs as written, but believe the VRFs should be changed. Also, CIP-004-6 VSL/VRF is provided at requirement subpart level, while the revisions summarize at requirement level. Expanding to make CIP-004 R6 to indicate VSL/VRF at requirement subpart level might be more helpful.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment
Request clarification that violating is at the CIP-004 Part level (6.2) not the items beneath Part 6.2 Request clarification that violating is at the CIP-011 Part level (1.3) not the items beneath Part 1.3

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
Puget Sound Energy supports the comments of EEI.

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 adding a lower VSL to CIP-011 R2 for not having a documented process, and a High VSL for not following the documented process and releasing or disposing of a BCA with accessible BCSI. The enforcement of R2 is not the same as the enforcement of R1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The VSLs for CIP-004-7 R6 and CIP-011-3 R1 do not adequately reflect the severity of a possible violation. For example, failure to properly identify BCSI could result in a high reliability risk. But since this would only be a violation of one part of CIP-011-3 R1 the VSL assigned would be “Lower.” This does not adequately assess the severity of the violation. This is especially true of CIP-011-3 R1 where Parts 1.2, 1.3 and 1.4 apply to BCSI as identified in Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the Comment Form submitted by EEI	
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	
Southern agrees the revisions to VSL/VRF for CIP-004 and CIP-011 are aligned properly based on the revisions in the respected Standards and Requirements.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
NVE supports the new and revised VSL/VRF descriptions	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E has no comments on the revised VSL/VRF's.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

PAC agrees with the new and revised VSL/VFR desciptions.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees the VSL/VRF matrix reflects accurately.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
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	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
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	

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	

Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing an 18-month implementation plan. Do you agree to the proposed timeframe?

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy would like a 24-month implementation plan to allow for contract revisions for vendors who are storing and analyzing data.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

These modifications create no significant new compliance requirements, but instead add flexibility and clarity for the Responsible Entities. A shorter time window, such as six months, would be more appropriate.

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

TVA does not believe 18 months is sufficient time to conduct required evaluation and implementation of required controls and associated processes. Suggest extend to 36 months.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month implementation plan to allow entities flexibility to determine the appropriate implementation actions.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Since the proposed changes to CIP-004 and CIP-011 revolve around the use of vendor services, the time to implement will be influenced by whether or not an organization uses or is planning to use vendor services to store, utilize, or analyze BCSI and if so, whether they have proactively implemented any of these controls. In either case, BPA believes 24 months is the minimum necessary due to the need for implementing or modifying contract language.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The material changes requiring incremental work are in relation to vendor services per CIP-011-2 R1.3. The requirements need clarity as to whether the controls are intended for net new engagements with vendor service providers as of the effective date of the standard or if it applies to pre-existing vendor service providers. There are several other clarity issues that need to be addressed in the standard requirements as per comments BC Hydro provided to the other questions posed by the SDT in this survey.	
Likes 0	
Dislikes 0	

Response
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh
Answer No
Document Name
Comment
N&ST's response to this question is based on our objections to the proposed revisions to CIP-004 and CIP-011.
Likes 0
Dislikes 0
Response
Andrea Barclay - Georgia System Operations Corporation - 4
Answer No
Document Name
Comment
Giving due consideration to the likelihood that Responsible Entities will need to revise their existing BCSI programs to manage such information based on each individual piece of BCSI, instead of based on storage locations or repositories, GSOC would respectfully suggest an implementation period of 24 months.
Likes 0
Dislikes 0
Response
David Jendras - Ameren - Ameren Services - 3
Answer No
Document Name
Comment
We recommend extending the implementation period to 24 months.
Likes 0
Dislikes 0
Response

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO-NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management	
Answer	No
Document Name	
Comment	
Since the intent of these changes is to allow for the use of cloud services, the IRC SRC recommends the SDT consider a phased implementation with mandatory compliance at the end of 18 months – following the concepts from the CIP-002-6 implementation plan. This would allow for a quicker adoption where and when possible for entities that choose to adopt cloud services in this capacity.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Please provide additional guidance on what is required for existing vendors with provisioned BCSI access. This will be helpful in determining implementation requirements.	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO is in support of the below IRC SRC comments: Since the intent of these changes is to allow for the use of cloud services, the IRC SRC recommends the SDT consider a phased implementation with mandatory compliance at the end of 18 months – following the concepts from the CIP-002-6 implementation plan. This would allow for a quicker adoption where and when possible for entities that choose to adopt cloud services in this capacity.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Alliant Energy agrees with the MRO NSRF's comments supporting an 18-month implementation period as a “not to exceed.” That said, we request the Standard Drafting Team (SDT) allow for implementation flexibility, i.e. so entities who are able and would like to move to the new version more quickly than 18 months can do so.	
Likes 0	
Dislikes 0	
Response	
Kayleigh Wilkerson - Lincoln Electric System - 5, Group Name Lincoln Electric System	
Answer	No
Document Name	
Comment	
LES supports an 18-month implementation period as a “not to exceed.” That said, we request the Standard Drafting Team (SDT) allow for implementation flexibility, i.e. so entities who are able and would like to move to the new version more quickly than 18 months can do so.	
Likes 0	

Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PAC agrees with the proposed timeframe.	
Likes 0	

Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment
PG&E believes the 18 month implementation plan is appropriate for the modifications.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment
MPC agrees with an 18-month implementation timeline. MPC also requests ERO guidance regarding early implementation of CIP-004-7 and CIP-011-3. An entity should be permitted to implement procedures to meet compliance with the revised requirements and not be held to previous requirements that are due to be retired upon the enforceable date of project 2019-02 when implementing such changes prior to the enforceable date.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	Yes
Document Name	

Comment
Recognizing that each entity is situated differently,the proposed 18 months is enough for AEP, since this will not result in any major changes to processes.

Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We support NPCC comments: For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes

Document Name	
Comment	
NVE supports an 18-month implementation period.	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
This is a critical during purchase of an entity with little time to implement the needed requirements.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
For quicker adoption when possible, per Entity phased adoption is desirable. Recommend a phased implementation with mandatory compliance at the end of 18 months – following concepts from the CIP-002-6 implementation plan Request clarification on what is the correct forum (other than the SDT) for discussing implementation plans?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the 18-month implementation plan proposed by the SDT.	
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	
Southern Company agrees the 18-month implementation plan is sufficient.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the Comment Form submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
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	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
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	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
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	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

6. The SDT proposes that the modifications in CIP-004 and CIP-011 meet the project scope in a cost-effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost-effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Clarity is needed to meet the project scope in a cost-effective manner. If encryption for BCSI stored in the cloud is an effective requirement even if the written requirement is more general, that is difficult for entities to follow and know they are compliant. It introduces compliance risk if entities make decisions based on an unclear requirement, and entities may think they are saving money by implementing a non-technical solution but that could backfire if a technical solution is actually required to be sufficient.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the Comment Form submitted by EEI

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Due to the endless possibilities of 3rd party storage solutions/vendor services for storage, we do not feel CIP-011 R1.3 is necessary and is exceedingly burdensome. If the currently written controls in R1.4 are implemented, the electronic technical mechanisms are sufficient to protect BCSI from unauthorized access.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO is in support of the IRC SRC comments:

The costs to implement the changes cannot be calculated as the standards are currently written; however, there are several areas where proposed modifications unnecessarily increase cost. We would require a better understanding of the term “provisioning” and the context of how the concepts outlined in both standards would apply in a use case where third party providers of services are going to be used to store or process BCSI information.

In the spirit of cost-effectiveness, the IRC SRC respectfully requests the SDT consider the following opportunities to consolidate requirements and/or eliminate duplication and overlap under CIP-004.

Introduction of “provisioning” not commensurate with cost – the proposed change from BCSI designated storage locations to personnel with provisioned access to BCSI creates significant administrative overhead for entities and is not commensurate with the security value achieved. The technical rationale identifying repositories for BCSI in the current standards vs “provisioned access” appears to be the same when you review information in the technical rationale narrative.

Opportunity to consolidate CIP-004 requirements - The addition of proposed new requirement, R6, would require entities to implement an access management program for ***BES Cyber System Information (BCSI; i.e. information)*** on par with the existing (and proposed continuation of) requirement, R4, to implement an access management program for ***BES Cyber Systems (BCS; i.e. assets)***, i.e., to identify, authorize and track provisioned and authorized personnel with access to BCSI - both hard-copy and electronic copy – at the entity’s managed location and at 3rd party storage locations (aka “cloud”) as well.

For entities using or considering a move to 3rd party cloud storage without encryption of BCSI (such as MS Office 365), entities will be required to obtain a list of 3rd party cloud personnel such as systems administrators with Administrative level privileges to systems which store an entity’s BCSI – which may also be replicated at multiple cloud data centers and multiple sets of personnel. This is not sustainable. To address this, and in keeping with the criteria of NERC’s Standards Efficiency Review, the IRC SRC proposes requirement R6 be consolidated into R4, so entities are only required to implement to a single access management program.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	
Comment	
We support NPCC Regional Standards Committee comments	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Business agreements with vendors requiring vulnerability and breach disclosures, as well as incident response, may not be cost-effective (or possible) to establish.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Based on our response to question 1, we believe that a more cost effective approach exists to enable use of third party services for storage and analysis of BCSI in a secure manner without introducing additional compliance burden on entities. The proposed revisions should not introduce additional requirements or compliance burden for those entities that do not plan to utilize third party services for storage or analysis of BCSI. In addition, we encourage a risk-based approach to address prevention of unauthorized access to BCSI while stored in third party environment or being processed by third-party. See our response to Question 3. A "cost-effective" approach would be for NERC to agree to rely on independent audit reports (eg SOC2 Type2)	

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management

Answer	No
Document Name	

Comment

The costs to implement the changes cannot be calculated as the standards are currently written; however, there are several areas where proposed modifications unnecessarily increase cost. We would require a better understanding of the term “provisioning” and the context of how the concepts outlined in both standards would apply in a use case where third party providers of services are going to be used to store or process BCSI information.

In the spirit of cost-effectiveness, the IRC SRC respectfully requests the SDT consider the following opportunities to consolidate requirements and/or eliminate duplication and overlap under CIP-004.

Introduction of “provisioning” not commensurate with cost – the proposed change from BCSI designated storage locations to personnel with provisioned access to BCSI creates significant administrative overhead for entities and is not commensurate with the security value achieved. The technical rationale identifying repositories for BCSI in the current standards vs “provisioned access” appears to be the same when you review information in the technical rationale narrative.

Opportunity to consolidate CIP-004 requirements - The addition of proposed new requirement, R6, would require entities to implement an access management program for ***BES Cyber System Information (BCSI; i.e. information)*** on par with the existing (and proposed continuation of) requirement, R4, to implement an access management program for ***BES Cyber Systems (BCS; i.e. assets)***, i.e., to identify, authorize and track provisioned and authorized personnel with access to BCSI - both hard-copy and electronic copy – at the entity’s managed location and at 3rd party storage locations (aka “cloud”) as well.

For entities using or considering a move to 3rd party cloud storage without encryption of BCSI (such as MS Office 365), entities will be required to obtain a list of 3rd party cloud personnel such as systems administrators with Administrative level privileges to systems which store an entity’s BCSI – which may also be replicated at multiple cloud data centers and multiple sets of personnel. This is not sustainable. To address this, and in keeping with the criteria of NERC’s Standards Efficiency Review, the IRC SRC proposes requirement R6 be consolidated into R4, so entities are only required to implement to a single access management program.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
NV Energy does not agree. The modifications as proposed by the SDT do not meet the project scope in a cost-effective manner. These modifications depend on established and/or modified vendor relationships that are being addressed outside of scope. This goes beyond the scope identified by the FERC Order for CIP-004 & CIP-011 in Project 2019-02. Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices. The new language in CIP-011 could result in required audits of third parties. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties compliance to the requirements, thus requiring undue burden on the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
The SDT needs to provide a cost/benefit analysis in order for us to determine if their proposal is cost effective. Also see SMUDs comments.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	

Comment
Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	No
Document Name	
Comment	

As discussed above, the proposed revisions increase the scope of applicability, ambiguity, compliance activities, and burden without the likelihood of an associated increase in reliability or security and with the potential to create a security gap related to the management and protection of BCSI. Moreover, the driver for these revisions do not impact all Responsible Entities. Accordingly, without appropriate backwards compatibility, Responsible Entities with existing, effective programs and no cloud or other third-party hosted services will be required to expend significant resources to ensure compliance.

This creates uncertainty and increases the burden of compliance on Responsible Entities for no ostensible enhancement to reliability or security. Taken together, the proposed revisions do not propose substantive enhancements to security or reliability that would justify the additional cost, resource, or compliance burden or risk for a large number of Responsible Entities.

Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	
Comment	

The current modifications to CIP-004 and CIP-011 do not meet the project scope in a cost-effective way. This is because there are elements of the changes to CIP-011 (see answer to question 7 below) that are supply chain risks that should be addressed in CIP-013 (Project 2019-03) rather than in Project 2019-02. Adding the level of Supply Chain Risk Management proposed within CIP-011 R1 Part 1.3, unecessarily adds significant implementation and cost burden. Inefficiencies will result from unecessary commingling of requirements for Projects 2016-02, 2019-02 and 2019-03.

Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	
Comment	

Due to the endless possibilities of 3rd party storage solutions/vendor services for storage, we do not feel CIP-011 R1.3 is necessary and is exceedingly burdensome. If the currently written controls in R1.4 are implemented, the electronic technical mechanisms are sufficient to protect BCSI from unauthorized access.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

It is N&ST's understanding that the primary goal of this project is to clarify requirements to prevent unauthorized access to BCSI while "in storage" in order to facilitate the use of 3rd-party storage solutions, including cloud-based services. If that understanding is correct, N&ST believes total rewrites of long-standing Information Protection Program and BCSI storage location access management requirements are neither necessary nor desirable.

N&ST believes adding a single, simply-worded requirement to either CIP-004 or CIP-011, stating that all "designated storage locations" must have documented technical controls that prevent unauthorized access to BCSI, would be quite sufficient.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

Regarding CIP-011-3 R1 Part 1.3, the terminology for the sub-parts do not add value to CIP-011. It is unclear what this terminology would require or what any of these terms mean, making them subject to broad and differing interpretation. This proposed requirement is a paperwork exercise that adds administrative burden without realizing security benefits. Auditability will be difficult and open to interpretation. For these reasons, MPC does not consider these changes to be cost-effective.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Technology and costs are ever evolving in this area and without NERC performing a cost benefit analysis it is impossibkle to judge the impact ofthis specific proposal.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E at this time cannot determine if the modifications are cost effective. PG&E would like to have an option to select Unknown, instead of just Yes and No.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5, Group Name NCPA	
Answer	No
Document Name	
Comment	
The SDT needs to provide a cost/benefit analysis in order for us to determine if their proposal is cost effective. Also see SMUDs comments.	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

As mentioned in question 1, changing the term from “designated storage locations” to “provisioned access” adds administrative work to update program documents and access tracking tools, without a commensurate increase in flexibility or security. CIP-011 R1.3 and R1.4 expand the scope of the SAR to include more than just cloud service providers and for medium impact without ERC. This is a significant expansion of scope that is not cost effective.

The existing versions of the CIP standards already take into consideration potential cloud service providers. One approach could be to allow current versions to remain effective, while offering the new versions to entities that want to implement them, as is being done with PRC-005 versions -1.1b and -6.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

As mentioned in question 1, changing the term from “designated storage locations” to “provisioned access” adds administrative work to update program documents and access tracking tools, without a commensurate increase in flexibility or security. CIP-011 R1.3 and R1.4 expand the scope of the SAR to include more than just cloud service providers and for medium impact without ERC. This is a significant expansion of scope that is not cost effective.

The existing versions of the CIP standards already take into consideration potential cloud service providers. One approach could be to allow current versions to remain effective, while offering the new versions to entities that want to implement them, as is being done with PRC-005 versions -1.1b and -6.

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No

Document Name	
Comment	
BC Hydro has insufficient information to determine how cost effective these modifications are. For additional details, please reference BC Hydro's comments to the other questions in this survey.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
This is very difficult to quantify across all of industry and various types of registered entities. If the language can be adjusted to account for non-electronic information storage locations, it has potential.	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Based on our response to question 1, we believe that a more cost effective approach exists to enable use of third party services for storage and analysis of BCSI in a secure manner without introducing additional compliance burden on entities. The proposed revisions should not introduce additional requirements or compliance burden for those entities that do not plan to utilize third party services for storage or analysis of BCSI. In addition, we encourage a risk-based approach to address prevention of unauthorized access to BCSI while stored in third party environment or being processed by third-party. See our response to Question 3.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

PAC does not agree. The modifications as proposed by the SDT do not meet the project scope in a cost-effective manner. These modifications depend on established and/or modified vendor relationships that are being addressed outside of scope. This goes beyond the scope identified by the FERC Order for CIP-004 & CIP-011 in Project 2019-02. Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices.

The new language in CIP-011 could result in required audits of third parties. CIP-013 doesn't require audits of vendor performance and adherence, where CIP-011 without similar exception would require these types of verifications for compliance. This is beyond the scope of the NERC CIP Standards to audit external third parties compliance to the requirements, thus requiring undue burden on the Responsible Entity.

Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	

As our comments in question 1, changing the term from "designated storage locations" to "provisioned access" adds administrative workload to update program documents and manage additional access to BCSI that is not manageable without an automated tool. We suggest using BCSI Repository approach to manage BCSI access as our comments in question 1. By using this approach, there is no additional cost for the ongoing compliance and the CIP-006 Part R16. 4.1 we suggest will address the cloud storage third-party access to BCSI.

Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

To minimize churn among standard versions, Reclamation recommends the SDT take additional time to coordinate the modifications in CIP-004-7 and CIP-011-3 with other existing drafting teams for related standards. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. NERC should foster a standards development environment that will allow entities to fully implement technical compliance with current standards before moving to subsequent versions. This will provide entities economic relief by better aligning the standards for overall improved reliability and by reducing the chances that standards will conflict with one another.

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

Under the existing version of the standards entities are already required to apply protection mechanisms to BSCI when shared. If requirement R1.3 remains it should not be applied retroactively to vendors.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino

Answer	No
Document Name	

Comment

The current approach would be resource intensive and difficult to manage. Many of the new requirements are also vague and broad. This could make it very difficult to come up with solutions to meet the requirement and may cost much more to implement than it would if the requirements and measures were clearer. Given the ambiguity, it is hard to imagine how the regional entities will interpret the requirements and how that would impact the implementation.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree. It is not clear the extent of changes that may be necessary to existing methods that are already effectively protecting BCSI and to what extent those changes will result in additional risk reduction.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
As written, R1.4 and R1.5 will apply to all vendors that also may utilize or analyze BCSI. This would mean that entities would have to utilize resources to identify/assess risks (R1.4) and would be required to develop/purchase/implement tools to ensure that at least one or more documented electronic technical mechanisms to protect BCSI (R1.5). While this makes sense when utilizing third-party solutions such as cloud services, these extra requirements for vendors that simply need to access physical or electronic documentation containing BCSI or that utilize this type of information onsite on a periodic basis appears unnecessary and costly to implement.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
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	
Southern has no comments on the project scope cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3	
Answer	Yes
Document Name	
Comment	
Again, recognizing that each entity is situated differently,the proposed revisions can likely be implemented by AEP in a cost effective manner, since this will not result in any major changes to processes.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The cost to implement will grow quickly with unclear requirements that lead to Responsible Entity concerns of proper interpretation. We would not say these are cost-effective at this time.	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF	
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	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kyle Hussey - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
No position.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	
Document Name	
Comment	
SDG&E has no comment on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response
Kinte Whitehead - Exelon - 3
Answer	
Document Name	
Comment
Exelon has elected to align with EEI in response to this question.
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	
Document Name	
Comment
Texas RE does not have comments on this question.
Likes 0	
Dislikes 0	
Response
Daniel Gacek - Exelon - 1
Answer	
Document Name	
Comment
Exelon has elected to align with EEI in response to this question.
Likes 0	
Dislikes 0	
Response

David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

7. Provide any additional comments for the standard drafting team to consider, if desired.	
Kjersti Drott - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
Technical rationale for CIP-011, part 1.4, implies there would always be the state "use" in all vendor solutions. However, in Tri-State's experience that is not always the case, and also depends on the individual's interpretation of what "use" of BCSI means. A common example where there would not be "use" in the cloud is backup storage. (Where the data is sent already encrypted and in order to use it (aka restore) has to be called back to the customer's premises to be unencrypted.) Recommend the SDT remove "use", or instead change the entire paragraph to refer to the lifecycle of the data from transit to disposal.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
none at this time, thank you.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 4	
Answer	
Document Name	
Comment	
The language is not clear on whether existing vendors will be subject to the new R1.4 and R1.5 requirements or if this will apply only to new vendors after the future enforcement date.	

The R1.4 language "identify and assess" is similar to CIP-013, which entities are finding requires a significant amount of resources to approrpriately comply with.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 6, 3, 5; - Joe Tarantino	
Answer	
Document Name	
Comment	
Granting access to individual pieces of information is not cost effective, would be resource intensive, and is not in line with industry best practices. The approach of managing access to repositories was a more practical approach and was more manageable as well.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	

I support the draft CIP-004-7 Standard, however there sonsistent use of defined terms could be implemented. BES Cyber System Information is established as the anacronym (BCSI) in R2.1, yet it is not used in R6, M6, or Table R6 title.

Conducting CIP-013 vendor risk assessments is a new process for many entities, it would just add additional confusion to have risk assessment requirements in standards other than CIP-013. The risk assessment required by draft Standard CIP-011-3 R1.3 should be omitted and moved to CIP-013.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

The NIST framework adequately addresses these Standards as they pertain to all BES Cyber Systems. The NIST framework is sufficient for guiding federal entities' security efforts pertaining to the Bulk-Power System, rather than creating duplicative requirements in the CIP standards. NERC should leverage and incorporate the existing NIST framework, instead of creating additional, identical requirements in the form of CIP standards. Additional, identical requirements create an administrative burden without improving overall security posture, thereby creating the potential for security failures because of the required inefficient use of resources.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	
Document Name	

Comment

We suggest removing CIP-011 Part 1.3 and P1.4 as our comments in question 3. Define a BCSI Repository term in CIP-011 and use it for the BCSI access management in CIP-004. Given that BCSI must have a home, there is no access control basis unless a BCSI repository is identified.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Puget Sound Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
General comment - Request consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:.” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency. Request consistent redlines because the CIP-011 redline-to-last-approved is not consistent with the CIP-011 redline-to-last-posted	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
Please copy applicabilty and change where appropriate for each part, such as done in CIP-011 R1	

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	
Document Name	

Comment

1. CIP-011 R1.3 is more appropriate to be located in CIP-013.
2. CIP-004-7 addresses access management controls for BCSI in relation to Medium Impact with ERC BES Cyber Systems and associated EACMS and PACS; however, CIP-011-3 is broader in scope to include Medium Impact BES Cyber Systems and associated EACMS and PACS without limiting coverage to ERC only. Why is there a discrepancy?

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	
Document Name	

Comment

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	
Document Name	

Comment

CEHE noticed that CIP-004-7 Requirement R6 does not consider revocation when an individual is reassigned or transferred, in a similar way in which it is accounted for in Requirement R5 Part 5.2.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5, Group Name NCPA

Answer	
Document Name	

Comment

No.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E has no additional input.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	
Document Name	

Comment

Minnkota respectfully states that it is opposed to changing the CIP Standards Requirements table column from “Applicable Systems” to “Applicability”. This could also be confused with the Applicability in section A.4. of the standard. While we appreciate the SDT’s attempt to clarify that the requirement is applicable to BCSI about those systems, regardless of if it is stored in those same systems or elsewhere, we propose that this be done in the requirement language instead. We submit for the SDT’s consideration the following proposal:

CIP-004
6.1 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “Authorize based on need, as determined by
the Responsible Entity, provisioneding of access to BCSI pertaining to applicable systems,
except for CIP Exceptional Circumstances.”
6.2 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “Verify at least once every 15 calendar months that all provisioned access to BCSI pertaining to applicable systems:”
6.3 Remove “BCSI associated with:” in Applicability column. Change column heading back to Applicable Systems. Change requirement to “For termination actions, remove the individual’s ability to use provisioned access to BCSI pertaining to applicable systems . . .”

CIP-011
1.1 Remove “BCSI pertaining to:” in Applicability column. Change column heading back to Applicable Systems. Change Requirement to “Method(s) to identify BCSI pertaining to applicable systems.”
1.2 Revert Applicability column back to currently enforceable. Change Requirement to “Method(s) to protect and securely handle BCSI pertaining to applicable systems.”

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3

Answer	
Document Name	

Comment

No further comment.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

No aditional comments

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

We thank you for this opportunity to comment.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned about the applicability in CIP-004-7 R4 and R5, and the use of encryption as stated in CIP-011-3. Additionally, Texas RE is concerned with the removal of key management in CIP-011-3. Regarding applicability, Texas RE recommends the standard drafting team (SDT) update the Applicable Systems columns in CIP-004-7 R4 (Parts 4.1-4.3) and R5 (Parts 5.1-5.4), to

Medium Impact BES Cyber Systems and their associated:

1. EACMS;
2. PACS; and
3. PCAs.

Since CIP-011-3 Parts 2.1 and 2.2 includes EACMS, PACS, and PCA, this change would align CIP-004-7 better with CIP-011-3 as well as improve an overall security posture for access management and revocation.

Regarding encryption, Texas RE continues to be concerned that entities could simply use the bare minimum encryption controls in accordance with CIP-011-3 R1.4. Neither CIP-004 nor CIP-011 contain requirement language specifying a minimum acceptable level of encryption where encryption is used. The absence of enforceable language results in any encryption algorithm at any key strength, including those algorithm and key strength combinations that have been determined to not be sufficiently strong, meeting compliance with this requirement as it is written. This may result in inconsistent enforcement of this requirement across the regions.

Texas RE suggests writing additional Part to CIP-011-3 Requirement R1:

Part 1.5 – For those methods identified in Part 1.4 that use encryption, utilize an encryption key strength of at least 128 bits.

This language is consistent with the NIST framework for medium-impact information and does not mandate the use of encryption. If encryption is used, however, it provides clear criteria as to what level of encryption is considered acceptable. The inclusion of minimal key strength criteria also squares with FERC's observations in its 2018 Staff Report, Lessons Learned from Commission-Led CIP Reliability Audits that select entities could improve their security posture by enhancing their encryption key strength.

Regarding key management, Texas RE is concerned with the removal of key management process(es) in CIP-011-3, Requirement R2, part 2.1. Key management is an important part of encryption and reduces the risk of unauthorized electronic access. Key management is also an important control when implementing third-party cloud service providers. If personnel have access to the encryption keys, they have electronic access to BCSI.

Texas RE has the following additional comments:

- Texas RE inquires as to the difference between the terms “provisioning of access” and “provisioned access”, which are used in CIP-004-7 R6 and the term “access”, which is used in R4 and R5.
- In the measure for CIP-011-3 R1 Part 1.3, Texas RE recommends changing “or” to “and”. Vendor certification alone is insufficient to verify vendor controls. Entities should have vendor certification and Registered Entity verification of vendor controls.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

ATC thanks the SDT for mindfully approaching the directives of this FERC Order so as to enable the CIP Standards for emerging technologies like off-premises BCSI cloud solutions/platforms, while maintaining backwards compatibility for on-premises BCSI solutions. Permitting the CIP Standards to stall and lag behind emerging/advancing technology disincentivizes the growth and maturity of our most critical infrastructure; which in and of itself breeds a security and reliability risk. Thank you also for the continued investment in the supporting materials like IG and TR; this truly helps provide a common understanding.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA agrees with the CIP-011 R1 Parts 1.1, 1.2 and 1.4 revisions. Requirement 1 Part 1.3 is a supply chain risk management requirement and CIP-011 should address only information security. The R1, Part 1.3 is a supply chain risk management provision that is more aptly dealt with in CIP-013. The language included in CIP-011 is not intended to require technical controls supporting the management of supply chain risk.

Public power finds the that current language of CIP-013 would provide the necessary clarity to implement the vendor assessment practices suggested in R1, Part 1.3. While the measures do provide some guidance, the measures are not part of the requirement language in R1, Part 1.3. The R1, Part 1.3 proposed language reads like a new requirement rather than something that complements CIP-013 practices.

The RI, Part 1.3 language suggests a gap that needs to be addressed in CIP-013. Attempting to address the risk inappropriately in CIP-011 would only set up future corrections.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	
Document Name	

Comment

Support the MRO-NSRF comments.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - 4 - NPCC,SERC,RF

Answer	
Document Name	

Comment

Better detail and clarifications are needed throughout multiple sections of the document.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management

Answer	
Document Name	

Comment

General comment – The IRC SRC requests consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

CIP-011 Part 1.3’s requirement includes “implement risk management method(s).” However the corresponding measures says “Implementation of the risk identification and assessment method(s) (1.3).” Consistency between the requirement and measure would reduce the risk of confusion. We would prefer the use of the terms “risk identification and assessment” as opposed to “risk management.” Risk management is generally understood to include many things. Request consistent redlines because the redline-to-last-approved is not the same redline-to-last-posted for CIP-011.

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1. To address this, the IRC SRC requests the SDT consider incorporating any necessary provisions into CIP-013.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	

Comment

General comment - Request consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:.” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

Request consistent redlines because the CIP-011 redline-to-last-approved is not consistent with the CIP-011 redline-to-last-posted

Since technological solutions are often the answer to the various challenges of the electrical industry, there is a tendency to resort to cloud computing solutions to accelerate deployment and reduce costs. It therefore appears important to us, in order to reduce cybersecurity risks to a minimum while ensuring the flexibility required by maintaining the reliability of the Bulk Electric System that NERC focus on adapting the CIP Reliability Standards to cloud computing environments. Exploring ways to integrate certifications (i.e. FedRamp, or Soc II Type 2) will be essential to permit compliance certification with the CIP requirements by various cloud providers. This support would prevent entities from needing to carry out isolated proceedings with suppliers, which may be inconsistent across industry.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	
Document Name	

Comment

CIP-011 Requirement 1.3 does not cleary identify what the requriment is. The measure is providing the clarity.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC

Answer	
Document Name	
Comment	

CAISO is in support of the below IRC SRC comments:

General comment – The IRC SRC requests consistent language in the (CIP-011) Measures. Parts 1.1, 1.2, 2.1, and 2.2 start with “Examples of acceptable evidence include, but are not limited to, the following:” Parts 1.3 and 1.4 start with “Examples of acceptable evidence may include, but are not limited to, dated documentation of the following:.” Part 1.3 is consistent with other Standards. Next, some Parts explicitly end each bullet with “or.” Some Parts are silent on how to read their bullets (or vs and). Request explicit consistency.

CIP-011 Part 1.3’s requirement includes “implement risk management method(s).” However the corresponding measures says “Implementation of the risk identification and assessment method(s) (1.3).” Consistency between the requirement and measure would reduce the risk of confusion.

We would prefer the use of the terms “risk identification and assessment” as opposed to “risk management.” Risk management is generally understood to include many things.

Request consistent redlines because the redline-to-last-approved is not the same redline-to-last-posted for CIP-011.

The standards drafting team has not provided enough justification for the new CIP-011-3 R1.3 and 1.4 vendor management requirements. The existing CIP requirements already require protection of BCSI, including BCSI stored, analyzed and used by vendors. The drafts would require almost the same level of protections as those required for BES Cyber Assets in CIP-013-1. To address this, the IRC SRC requests the SDT consider incorporating any necessary provisions into CIP-013.

Finally, the wording of CIP-004-7, Part 6.2 expands the scope of the 15-month review (i.e. to verify the *need* for continued access) to include the quarterly review performed under Part 4.2 (i.e. to verify that provisioned access is *authorized*). To eliminate duplication, Part 6.2 should be reworded to mirror that of CIP-004-6, Part 4.4 (i.e. to verify that access is correct and necessary for performing assigned work functions).

Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We thank you for this opportunity to comment.	
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	
Southern does not have any additional comments other then those stated in the previous questions.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 1, 5, 3, 6; Bryan Taggart, Westar Energy, 1, 5, 3, 6; Derek Brown, Westar Energy, 1, 5, 3, 6; Grant Wilkerson, Westar Energy, 1, 5, 3, 6; - Douglas Webb, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2019-02 BES Cyber System Information Access Management

Summary Response to Comments | Draft 3

Background

Project 2019-02 BES Cyber System Information Access Management (BCSI) enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the project seeks to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

The Project 2019-02 BCSI standard drafting team (SDT) revised Reliability Standards CIP-004 and CIP-011 and reviewed the Glossary of Terms Used in NERC Reliability Standards pertaining to requirements addressing BCSI. The 45-day comment period was August 6 through September 21, 2020. There were 68 sets of responses, including comments from approximately 175 different people from approximately 111 companies representing 10 of the Industry Segments as shown in the table on the following pages. Based on these comments, the SDT has made proposed revisions to CIP-004 and CIP-011. Summary responses have been developed to address the comments.

CIP-004 Revisions

The SDT appreciates all comments submitted regarding the CIP-004 draft standard. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Provisioned access, provisioning, deprovisioning Concepts

Many commenters expressed concern about the phrase "provisioned access, provisioning, deprovisioning" within the CIP-004 standard. Some entities recommended the term be defined or the SDT modify the requirements to provide clarity. It was also acknowledged that the Technical Rationale (TR) does a great job explaining this term, but there is concern as the TR is not enforceable.

Thank you for your comments. The SDT determined that the term provision does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. The SDT made some modifications within the sub-requirements of CIP-004 in hopes to provide clarity around the requirements regarding provisioned access. Lastly, the SDT encourages industry to review the CIP-004-X Requirement R6 section of the TR document and use the described concepts and scenarios in written access management programs.

Storage Location

Some commenters requested that the SDT revert back to storage locations as seen in the previous approved standard. In addition, a commenter expressed conversations with the SDT have clarified that CIP-004-7 R6.1 was not intended to require provisioning of access to each individual piece of BCSI. The SDT explained that the language was written to accommodate a use case where the BCSI authorization attaches to the document so that the authorization follows the document when moved to various locations. However, the entity requested the SDT accommodate both circumstances where entities may fall under the use case scenario or may use designated storage locations for BCSI. A couple of entities expressed that the proposed language is more restrictive than objective based. Lastly, some entities are concerned that the current proposed language will not allow for backwards compatibility.

Thank you for your comments. The SDT determined that reverting back to storage locations would not be an appropriate path forward for BCSI modifications and would be a detriment for future cloud modifications to the CIP standards. The provision concept provides a clear path for BCSI and future modifications. While entities may find Requirement R6 to be more restrictive than objective, the SDT's focus is on BCSI and objective based for this specific requirement may bring more into scope than intended and would be outside the scope of this team. Lastly, using "Storage Locations" is just one method to identify and protect BCSI. The absence of "Storage Locations" does not preclude an entity from maintaining that approach as their method. Removing "Storage Locations" adds the needed flexibility for entities that want to use other approaches such as those that technologies would provide (e.g. Azure Information Protection (AIP)). The term "Storage Locations" is too prescriptive, and retention of that term encumbers the use of emerging technologies for entities that should have those methods as an option. The SDT updated the Technical Rationale (TR) with an explanation of how "provisioned access" is backwards compatible with "designated storage locations", while still also allowing certain protections (i.e. encryption) at the file level rather than all entities having to limit this to specific locations.

Applicability

Many commenters requested that the SDT revert the "Applicability" column language back to "Applicable Systems" language.

Thank you for your comments. The SDT agrees and modified the applicability column language back to "Applicable Systems."

Clarify requirements for managing provisioned access utilizing third-party solutions.

There were concerns expressed about the lack of clarity regarding Requirement R6 and what provisioned access means and the lack of clarity regarding using cloud vendors.

Thank you for your comments. The SDT reviewed requirement R6 and agrees that some modifications are necessary. Please see the modifications made to CIP-004, Requirement R6.

Requirement R6 and Subparts 6.1 and 6.2

A couple of entities expressed that Requirement R6 and its subparts do not provide clarity. The entity stated that the intent of these requirements is to manage access when utilizing third-party solutions since it doesn't explicitly make that statement. The phrase "provisioning of access" does not necessarily imply "when utilizing third-party solutions."

Thank you for your comments. The SDT chose not to differentiate between entity and third-party because the requirement applies to each individual (whether employee or non-employee) and not the hiring company nor the infrastructure solution (whether on-prem or off-prem). The intent is to keep the requirements objective and agnostic of the workforce and infrastructure. Thereby permitting entities flexibility to adapt their program to their changing environment and workforce while still meeting the security objectives and without having to revise the requirements to catch up.

Many entities expressed that management of provisioned access to BCSI, when utilizing third-party solutions, needs to be clarified. Requirement R6, part 6.1 states that entities are required to "authorize provisioning of access to BCSI based on need." This could be read to mean, among other things, that entities are required to authorize someone to provision access to BCSI, provision access to all BCSI (i.e. requiring a provisioning authorization for each piece of BCSI), or a variety of other interpretations. To resolve this issue, EEI suggests aligning the language of Requirement R6, part 6.1 to Requirement R4, part 4.1 by adding the phrase "Process to", which would place the responsibility on the entity to define its process. Additionally, if process is added to the Requirement, the entity proposes adding an example such as "A documented process used to define provisioned access to BCSI."

Thank you for your comments. The SDT's intent in this context is for "provisioned access" to be limited to what an entity's program must do (authorize, verify, and revoke) thereby permitting the entity to determine "how" provisioning occurs. "Provisioned access" is a noun that the represents the result of executing the program so the security objective is met, and not a verb relating to how provisioning/deprovisioning occurs (the provisioning/deprovisioning actions and processes are up to the entity to design within the parameters of the objective.)

An entity expressed that the addition of Requirement R6 for CIP-004 makes it extremely difficult for entities to control access to BCSI. This is because of the requirement to provision access to individual pieces of information rather than provisioning access to where information is being stored (Storage locations).

Thank you for your comments. The SDT's modifications do not prescribe how to meet the security objective, nor does it prescribe controls at the individual document level. Using "Storage Locations" is just one method that could continue to be used within an entity's access management program when it comes to authorization, verification, and revocation of access for identified BCSI. The absence of "Storage Locations" does not preclude an entity from maintaining that approach as their method. The term "Storage Locations" is too prescriptive (Removing "Storage Locations" provides flexibility), and retention of that term encumbers the use of emerging technologies and approaches for entities that should have those methods as an option in addition to (not instead of) the current method.

Some entities requested clarification whether third-party access should be managed on an individual or team basis.

Thank you for your comments. The SDT maintained objective language at the requirement level to provide entities the flexibility to define "how" access is managed. Ultimately, regardless of whether the access is provisioned on an individual or team basis, the authorization records must trace back to each individual.

There was expressed concern from some entities that Requirement R6 Part 6.1 mirrors Requirement R4 Part 4.1.

Thank you for your comments. The SDT does not agree that the new Requirement R6 Part 6.1 mirrors Requirement R4 Part 4.1. CIP-004 Requirement R4 focuses on Access Management Programs and CIP-004 Requirement R6 focuses on authorizing, verifying, and revoking provisioned access. The similarities of these requirements were intentionally drafted. The security concepts and values are comparable, but the applicability is different. While an entity may leverage one program to support the other, or produce similar evidence to demonstrate compliance, the difference between them is the existing set of requirements should focus on BCS Access Management, and the proposed R6 on BCSI Access Management.

A couple of entities expressed concerns about a security gap – Differentiate between state protections for physical versus electronic BCSI protections.

Thank you for your comments. The SDT does not foresee a security gap. The CIP-004 standard Requirement R6 is intended to assure personnel (employee and non-employee) authorization, verification, and revocation of provisioned access to electronic or physical BCSI, whereas CIP-011 Requirement R1 covers the identification methods for the BCSI itself and the administrative or technical methods (whether electronic or physical protections) used to assure confidentiality of the BCSI. The SDT determined that, when a Responsible Entity designates material (whether physical or electronic) as BCSI, it is considered BCSI regardless of state (storage, transit, or in use) and requires protection under the information protection program.

Some entities requested the SDT to leverage the language in the current CMEP Practice Guide. State "access and use" or "obtain and use" in the requirement instead of just "use". Also, incorporate "Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020."

Thank you for your comments. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear a two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI, and agrees this is important to incorporate. As a result, the SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. The SDT leveraged language from the CMEP Practice Guide to modify Requirement R6 where necessary. Please see updated modifications.

An entity expressed the wording "based on need" is not necessary within Requirement R6 Part 6.1.

Thank you for your comments. The SDT considered the wording "based on need" and determined it is imperative that the Responsible Entity have the authority to determine the business need. Removal of this language could expose entities to undue compliance risk if it is left subjective as to who determines business need. Additionally, "based on business need" is included in the current enforceable requirement. Removal of it could be perceived as materially changing or diluting the requirement that was written to achieve former FERC directives, or out of scope of the 2019-02 standard authorization request (SAR). As a result, the SDT chose to retain this language for ultimate clarity that business need is determined by the Responsible Entity.

An entity expressed that the "CIP Exceptional Circumstances" is not necessary for Requirement R6 Part 6.1.

Thank you for your comments. The SDT has identified use cases where it may not be reasonable to expect an entity to execute its authorization processes to provision BCSI access, particularly in the case of physical BCSI and physical access needs of first responders in situations of medical, safety, or other emergencies as defined by CIP Exceptional Circumstances.

An entity expressed that the measures in Requirement R6 Part 6.1 "Dated authorization records for provisioned access to BCSI based on need." The statement "based on need" is not necessary here. If it is, then be clear on the expectations that the evidence needs to document the business need.

Thank you for your comments. The SDT considered the consistency concern from the presence of "based on need" in the requirement and the way it had been used within the measure. For clarity, the SDT adjusted the bullet in the measures to provide meaningful examples of evidence for "business need".

Measures

An entity expressed concern that the CIP-004 Requirement R6 Part 6.2 measures are too detailed when referring to privileges. Many types of access to BCSI are binary, either you have it or you do not. Recommend the SDT remove the 3rd and 4th bullets in the measure so that an entity could simply verify that the access is still necessary and appropriate for their job.

Thank you for your comments. The SDT reviewed the measures and updated them by removing the third and fourth bullets.

An entity proposed using a third-party example in the measures for Requirement R6.

Thank you for your comments. The SDT wrote the measures to apply to internal or external personnel. For this reason, the SDT did not cite a specific third-party example.

CIP-011 Revisions

The SDT appreciates all comments submitted regarding the CIP-011 draft standard. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Many entities expressed concern regarding CIP-011 Requirement R1 Part 1.3 and 1.4. In addition, some entities expressed that backwards compatibility would be difficult with the additional burden these subparts place on entities. Lastly, many entities requested clarity around certain wording and language. (e.g., "utilizing", consistent language with the standards authorization request (SAR), etc.)

Thank you for your comments. The SDT removed Part 1.3 and 1.4 from the CIP-011 standard which should alleviate backwards compatibility concerns and consistency with the language from the SAR.

A few entities stated that the new Requirement R1 Part 1.3 should be housed in CIP-013.

Thank you for your comments. The SDT removed Requirement R1 Part 1.3. As far as moving it to CIP-013, that is outside the scope of this project. Anyone is welcome to submit a SAR. The forms are located on the NERC Standards Resources page (link).

An entity requested the SDT be consistent between requirements and measures within CP-011 Requirement R3 Part 1.3.

Thank you for your comments. The SDT removed Requirement R3 Part 1.3 from CIP-011 and ensures that future requirements and measures are closely reviewed for consistency.

An entity requested the SDT confirm redlines posted for ballot and comment are correct.

Thank you for your comments, our apologies for the confusion. The SDT ensures the standard's redline and clean versions align for the next posting.

Measures

An entity requested the SDT be consistent throughout the opening of the measures.

Thank you for your comments. The SDT agrees with this request and modified the measures accordingly.

Some entities expressed concern that the measures for CIP-011 Requirement R1 Part 1.2 could provide audit approach confusion and requested that additional examples be provided.

Thank you for your comments. The SDT modified Requirement R1 Part 1.2 to provide clarity and additional examples.

Technical Rationale

An entity expressed that the TR for CIP-011, part 1.4, implies there would always be the state "use" in all vendor solutions. However, in this entity's experience that is not always the case, and also depends on the individual's interpretation of what "use" of BCSI means. A common example where there would not be "use" in the cloud is backup storage. (Where the data is sent already encrypted and in order to use it (aka restore) has to be called back to the customer's premises to be unencrypted.) The entity recommended the SDT remove "use", or instead change the entire paragraph to refer to the lifecycle of the data from transit to disposal.

Thank you for your comments. The SDT removed CIP-011 Requirement R1 Part 1.4 from the standard; therefore, it has been removed from the TR.

Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs)

The SDT appreciates all comments submitted regarding the VRF and VSL parts of the standards. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

Many entities expressed concern that the VSLs do not adequately reflect the severity of a possible violation for CIP-004 and CIP-011 modifications.

Thank you for your comments. The SDT reviewed the VSLs and modified them based on comments received.

Any entity requested that the SDT consider updating the VRF for CIP-011 Requirement R1 and Requirement R2 from a medium to a high. The basis for these reasonings are (R1) on the possible extension of BCSI to cloud providers, and the fact that there have been significantly more sophisticated, and a greater volume of, attacks against the energy industry, especially through phishing; (R2) with known foreign ownership, control, or involvement in PC reclamation and recycling, and the focus of foreign adversaries trying to gain access, cause damage, or control the US Power grid.

Thank you for your comments. The SDT reviewed the VRFs for CIP-004 and CIP-011 and determined that the standard requirements and modifications do not directly affect the grid. Therefore, the VRFs should remain a medium.

Implementation Plan

The SDT appreciates all comments submitted regarding the 18-month proposed implementation plan. The SDT reviewed each comment carefully and made respective changes where clarity or examples were needed.

18-month Implementation

In general, a majority of commenters agreed with the 18-month implementation plan. Some entities suggested 24-months as a more appropriate timeframe with the option for early adoption. It was further explained in comments that 24-months would be appropriate based on the need to revise their existing BCSI programs, an entity working with a vendor service to store, utilize, or analyze BCSI to ensure the appropriate controls have been implemented, etc.

Thank you for your comments. The SDT determined that a 24-month implementation plan would be an appropriate timeframe based on the comments received. In addition, Project 2019-02 is working closely with Project 2016-02 Modification to CIP Standards towards a seamless transition as both projects aim to combine the implementation plans later this year for NERC Board adoption. The SDT also determined that an early adoption within the implementation plan would be an appropriate modification. The SDT has modified the implementation plan to allow entities 24-months for implementation or early adoption based on discussion and agreement made with the entity's respective Region.

A couple of entities mentioned that implementation would be difficult based on ambiguity and uncertainty around respective requirements.

Thank you for your comments. The SDT encourages entities to review the provided responses to the questions regarding those respective requirements.

A couple of entities mentioned phased-in implementation should be allowed.

Thank you for your comments. The SDT believes that 24-months should allow entities ample time, and a phased-in approach is not necessary. In addition, an option for early adoption was added to the implementation plan for entities who wish to adopt the modifications sooner.

Cost-effectiveness

The SDT appreciates all comments submitted regarding cost-effectiveness among the standard modifications. The SDT reviewed each comment carefully and made respective changes where needed.

Some entities expressed concern around scope of applicability, ambiguity, unclear requirements, administrative burden, uncertainty around the word provision and how it would be used with third-party providers, etc.

Thank you for your comments. The SDT encourages entities to review the modifications made throughout the CIP-004 and CIP-011 Reliability Standards. In regards to the word provisioned, please see the TR document as it provides a thorough explanation of the word/term provision or provisioned access. This is a commonly used term among technical experts and should not cause a cost-effectiveness constraint on entities. Please also refer to the SDT's explanation under the title "Provisioned Access."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through September 21, 2020

Now Available

A 45-day formal comment period for **Project 2019-02 BES Cyber System Information Access Management** is open through **8 p.m. Eastern, Monday, September 21, 2020** for the following Standards and Implementation Plan:

CIP-004-7 - Cyber Security - Personnel & Training
CIP-011-3 - Cyber Security - Information Protection
Implementation Plan

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Linda Jenkins regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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

Additional ballots for the standards and implementation plan, along with non-binding polls for each associated Violation Risk Factors and Violation Severity Levels will be conducted **September 11–21, 2020**.

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

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2019-02 BES Cyber System Information Access Management" in the Description Box. For more information or assistance, contact Senior Standards Developer, Latrice Harkness (via email) or at 404-446-9728.

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
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 AB 2 ST
Voting Start Date: 9/11/2020 12:01:00 AM
Voting End Date: 9/21/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 232
Total Ballot Pool: 279
Quorum: 83.15
Quorum Established Date: 9/21/2020 2:58:09 PM
Weighted Segment Value: 32.8

Actions

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	79	1	20	0.328	41	0.672	0	5	13
Segment: 2	2	0.2	0	0	2	0.2	0	0	0
Segment: 3	60	1	18	0.375	30	0.625	0	4	8
Segment: 4	17	1	5	0.417	7	0.583	0	0	5
Segment: 5	69	1	17	0.327	35	0.673	0	5	12
Segment: 6	45	1	9	0.29	22	0.71	2	3	9
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.4	1	0.1	3	0.3	0	2	0
Totals:	279	5.6	70	1.837	140	3.763	2	20	47

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Third-Party Comments
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Third-Party

					Comments
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Third-Party Comments
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		None	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green		Negative	Third-Party Comments
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments

4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Third-Party Comments
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A

1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
3	Manitoba Hydro	Karim Abdel-Hadi		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		None	N/A

1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz	Abstain	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A

1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Negative	No Comment Submitted
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Negative	Third-Party Comments
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	None	N/A
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi	Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu	Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck	Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy	Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger	Affirmative	N/A
1	Platte River Power Authority	Matt Thompson	Negative	Comments Submitted

5	JEA	John Babik		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
					Third-Party

1	PPL Electric Utilities Corporation	Preston Walker		Negative	Comments
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		None	N/A
5	Enel Green Power	Mat Bunch		Abstain	N/A
					No Comment

6	Xcel Energy, Inc.	Carrie Dixon	Negative	Submitted
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz	Negative	Third-Party Comments
1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Xcel Energy, Inc.	Ray Jasicki	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Third-Party Comments
6	Snohomish County PUD No. 1	John Liang	Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Negative	Third-Party Comments
5	AEP	Thomas Foltz	Affirmative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Affirmative	N/A
6	AEP	JT Kuehne	Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski	Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	None	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson	Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Affirmative	N/A
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A

6	Duke Energy	Greg Cecil	Abstain	N/A
5	Duke Energy	Dale Goodwine	Abstain	N/A
3	Duke Energy	Lee Schuster	Abstain	N/A
4	National Rural Electric Cooperative Association	Paul McCurley	None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright	None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Abstain	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	Negative	Third-Party Comments
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	None	N/A
1	Evergy	Allen Klassen	None	N/A
3	Evergy	Marcus Moor	None	N/A
5	Evergy	Derek Brown	None	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	None	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 2 ST
Voting Start Date: 9/11/2020 12:01:00 AM
Voting End Date: 9/21/2020 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 228
Total Ballot Pool: 278
Quorum: 82.01
Quorum Established Date: 9/21/2020 3:01:23 PM
Weighted Segment Value: 23.06

Actions

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	79	1	12	0.197	49	0.803	0	5	13
Segment: 2	2	0.2	0	0	2	0.2	0	0	0
Segment: 3	59	1	9	0.196	37	0.804	0	4	9
Segment: 4	17	1	4	0.333	8	0.667	0	0	5
Segment: 5	69	1	13	0.255	38	0.745	1	4	13
Segment: 6	45	1	6	0.188	26	0.813	1	3	9
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	1	0.1	2	0.2	0	2	1
Totals:	278	5.5	45	1.268	162	4.232	2	19	50

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Third-Party Comments
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments

1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Negative	Third-Party Comments
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		None	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green		Negative	Third-Party Comments
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
					Third-Party

1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Third-Party Comments
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		None	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Negative	No Comment Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted

3	Platte River Power Authority	Wade Kiess		Negative	Comments Submitted
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted

3	Manitoba Hydro	Karim Abdel-Hadi	Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas	Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott	Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock	None	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz	Abstain	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted

5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Negative	Third-Party Comments
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	None	N/A
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted

5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Negative	Comments Submitted
5	JEA	John Babik		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	David Reinecke		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Negative	Third-Party Comments
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael	Negative	Comments

			Johnson		Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted

4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Negative	Comments Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	None	N/A
5	Enel Green Power	Mat Bunch	None	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	No Comment Submitted
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz	Negative	Third-Party Comments
1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Third-Party Comments
6	Snohomish County PUD No. 1	John Liang	Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Negative	Third-Party Comments
5	AEP	Thomas Foltz	Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Affirmative	N/A

6	AEP	JT Kuehne	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	None	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard	Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson	Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Abstain	N/A
5	Duke Energy	Dale Goodwine	Abstain	N/A
3	Duke Energy	Lee Schuster	Abstain	N/A
4	National Rural Electric Cooperative Association	Paul McCurley	None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright	None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Abstain	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	None	N/A
1	Evergy	Allen Klassen	None	N/A
3	Evergy	Marcus Moor	None	N/A
5	Evergy	Derek Brown	None	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	None	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management Implementation Plan AB 2 OT
Voting Start Date: 9/11/2020 12:01:00 AM
Voting End Date: 9/21/2020 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 222
Total Ballot Pool: 274
Quorum: 81.02
Quorum Established Date: 9/21/2020 3:09:50 PM
Weighted Segment Value: 50.49

Actions

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	78	1	29	0.483	31	0.517	0	5	13
Segment: 2	2	0.2	0	0	2	0.2	0	0	0
Segment: 3	58	1	25	0.568	19	0.432	0	4	10
Segment: 4	17	1	6	0.545	5	0.455	0	1	5
Segment: 5	67	1	29	0.58	21	0.42	0	5	12
Segment: 6	45	1	15	0.5	15	0.5	1	3	11
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	1	0.1	2	0.2	0	2	1
Totals:	274	5.5	105	2.777	95	2.723	1	21	52

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Third-Party Comments
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Third-Party Comments
1	Edison International - Southern California Edison	Jose Avendano		Negative	Third-Party

	Company	Mora			Comments
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Third-Party Comments
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		None	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Affirmative	N/A
6	Western Area Power Administration	Erin Green		Negative	Third-Party Comments
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Abstain	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Negative	Comments Submitted

1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Third-Party Comments
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		None	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Third-Party Comments
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A

5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		None	N/A
1	Lakeland Electric	Larry Watt		None	N/A
5	Lakeland Electric	Becky Rinier		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
3	Eversource Energy	Sharon Flannery		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Negative	Third-Party Comments
6	Muscatine Power and Water	Nick Burns	Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	Affirmative	N/A
5	Westar Energy	Derek Brown	Affirmative	N/A
6	Westar Energy	Grant Wilkerson	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas	Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Negative	Third-Party Comments
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	None	N/A
6	Portland General Electric Co.	Daniel Mason	None	N/A
1	Muscatine Power and Water	Andy Kurriger	Negative	Third-Party Comments

3	New York Power Authority	David Rivera		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A

3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
					Comments

3	Exelon	Kinte Whitehead	Negative	Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	None	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	No Comment Submitted
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz	Negative	Third-Party Comments
1	Georgia Transmission Corporation	Greg Davis	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Third-Party Comments
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Third-Party Comments
6	Snohomish County PUD No. 1	John Liang	Negative	Third-Party Comments
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Negative	Third-Party Comments
5	AEP	Thomas Foltz	Affirmative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Affirmative	N/A
6	AEP	JT Kuehne	Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski	Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	None	N/A

5	Seminole Electric Cooperative, Inc.	Mickey Bellard	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson	Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Affirmative	N/A
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Abstain	N/A
5	Duke Energy	Dale Goodwine	Abstain	N/A
3	Duke Energy	Lee Schuster	Abstain	N/A
4	National Rural Electric Cooperative Association	Paul McCurley	None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright	None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Abstain	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	None	N/A
1	Evergy	Allen Klassen	None	N/A
3	Evergy	Marcus Moor	None	N/A
5	Evergy	Derek Brown	None	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	None	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 Non-Binding Poll AB 2 NB
Voting Start Date: 9/11/2020 12:01:00 AM
Voting End Date: 9/21/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 210
Total Ballot Pool: 262
Quorum: 80.15
Quorum Established Date: 9/21/2020 3:09:27 PM
Weighted Segment Value: 32.08

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	72	1	12	0.273	32	0.727	14	14
Segment: 2	2	0.2	0	0	2	0.2	0	0
Segment: 3	59	1	13	0.361	23	0.639	12	11
Segment: 4	14	1	5	0.5	5	0.5	1	3
Segment: 5	64	1	13	0.333	26	0.667	12	13
Segment: 6	44	1	6	0.25	18	0.75	9	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.4	2	0.2	2	0.2	2	0
Totals:	262	5.6	51	1.917	108	3.683	51	52

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Comments Submitted

1	Edison International - Southern California Edison Company	Jose Avendano Mora		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		None	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A

1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Eversource Energy	Quintin Lee		Abstain	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A

3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
5	Lakeland Electric	Becky Rinier		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A

1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Negative	Comments Submitted
6	Muscatine Power and Water	Nick Burns	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A

6	Portland General Electric Co.	Daniel Mason		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
5	JEA	John Babik		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
		JULIE			

5	PPL - Louisville Gas and Electric Co.	HOSTRANDER		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

1	Exelon	Daniel Gacek	Negative	Comments Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	None	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Negative	Comments Submitted
5	AEP	Thomas Foltz	Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
6	AEP	JT Kuehne	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	None	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	Affirmative	N/A

8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Abstain	N/A
5	Duke Energy	Dale Goodwine	Abstain	N/A
3	Duke Energy	Lee Schuster	Abstain	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Abstain	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	None	N/A
1	Evergy	Allen Klassen	None	N/A
3	Evergy	Marcus Moor	None	N/A
5	Evergy	Derek Brown	None	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	None	N/A

[redacted]

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 Non-Binding Poll AB 2 NB
Voting Start Date: 9/11/2020 12:01:00 AM
Voting End Date: 9/21/2020 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 209
Total Ballot Pool: 263
Quorum: 79.47
Quorum Established Date: 9/21/2020 3:25:14 PM
Weighted Segment Value: 24.36

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	72	1	8	0.186	35	0.814	15	14
Segment: 2	2	0.2	0	0	2	0.2	0	0
Segment: 3	59	1	7	0.194	29	0.806	12	11
Segment: 4	14	1	5	0.5	5	0.5	1	3
Segment: 5	65	1	12	0.308	27	0.692	12	14
Segment: 6	44	1	5	0.217	18	0.783	10	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.3	1	0.1	2	0.2	2	1
Totals:	263	5.5	38	1.506	118	3.994	53	54

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters		Negative	Comments Submitted
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson	Barry Jones	Abstain	N/A
1	Edison International - Southern California Edison	Jose Avendano		None	N/A

	Company	Mora			
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		None	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Negative	Comments Submitted
6	Western Area Power Administration	Erin Green		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A

10	Midwest Reliability Organization	William Steiner		None	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Lisa Martin		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		Negative	Comments Submitted
5	San Miguel Electric Cooperative, Inc.	Lana Smith		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Eversource Energy	Quintin Lee		Abstain	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments

					Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Truong Le	Affirmative	N/A
3	Florida Municipal Power Agency	Dale Ray	Truong Le	Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	None	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
1	Tri-State G and T Association, Inc.	Kjersti Drott		Negative	Comments Submitted
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
5	Lakeland Electric	Becky Rinier		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
3	Eversource Energy	Sharon Flannery		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A

1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Negative	Comments Submitted
6	Muscatine Power and Water	Nick Burns	Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	Comments Submitted
3	Westar Energy	Bryan Taggart	Negative	Comments Submitted
5	Westar Energy	Derek Brown	Negative	Comments Submitted
6	Westar Energy	Grant Wilkerson	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz	Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Carey	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
1	Westar Energy	Allen Klassen	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	None	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Marty Hostler	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay	Negative	Comments Submitted

1	New York Power Authority	Salvatore Spagnolo	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson	None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte	Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Gail Golden	None	N/A
6	Portland General Electric Co.	Daniel Mason	None	N/A
1	Muscatine Power and Water	Andy Kurriger	Negative	Comments Submitted
3	New York Power Authority	David Rivera	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu	Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich	Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett	Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi	Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu	Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck	Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy	Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger	Affirmative	N/A
5	JEA	John Babik	Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason	Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke	Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff	None	N/A
6	Imperial Irrigation District	Diana Torres	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse	Negative	Comments Submitted
5	Public Utility District No. 1 of Chelan County	Meaghan Connell	Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry	Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding	Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein	None	N/A
1	NB Power Corporation	Nurul Abser	Abstain	N/A
				Comments

5	Dairyland Power Cooperative	Tommy Drea		Negative	Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
3	Portland General Electric Co.	Dan Zollner		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	Affirmative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments

				Submitted
6	Powerex Corporation	Gordon Dobson-Mack	Abstain	N/A
1	American Transmission Company, LLC	LaTroy Brumfield	None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert	Affirmative	N/A
5	New York Power Authority	Shivaz Chopra	Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Negative	Comments Submitted
3	Exelon	Kinte Whitehead	Negative	Comments Submitted
5	Exelon	Cynthia Lee	Negative	Comments Submitted
6	Exelon	Becky Webb	Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	None	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers	Negative	Comments Submitted
3	Bonneville Power Administration	Ken Lanehome	Negative	Comments Submitted
5	Bonneville Power Administration	Scott Winner	Negative	Comments Submitted
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang	Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Negative	Comments Submitted
5	AEP	Thomas Foltz	Negative	Comments Submitted
				Comments

1	AEP - AEP Service Corporation	Dennis Sauriol	Negative	Comments Submitted
6	AEP	JT Kuehne	Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski	Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	None	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps	None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Abstain	N/A
5	Duke Energy	Dale Goodwine	Abstain	N/A
3	Duke Energy	Lee Schuster	Abstain	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Abstain	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	None	N/A
1	Evergy	Allen Klassen	None	N/A
3	Evergy	Marcus Moor	None	N/A
5	Evergy	Derek Brown	None	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	None	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	None	N/A

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
10-day final ballot	May 2021
Board adoption	November 2021

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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:

All BES Facilities.

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

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-004-X.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

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

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

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

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

CIP-004-X Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.

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

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

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

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

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

CIP-004-X Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

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

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

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI. Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access within 15 calendar months of the previous training completion date. (2.3)	calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors,	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems,	quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were	quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			privileges were incorrect or unnecessary. (4.3)	incorrect or unnecessary. (4.3)		account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating	those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)			
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual,	electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the	access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not do so by the timeframe required in Requirement R6, Part 6.3.	timeframe required in Requirement R6, Part 6.3.		not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~August 2020~~
10-day final ballot	~~September~~ May 2021~~0~~
Board adoption	November 2021~~0~~

A. Introduction

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

2. **Number:** CIP-004-X~~7~~

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-X~~7~~:

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-002-5.1a identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-004-X~~7~~.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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" ~~or "Applicability"~~ column~~. The "Applicable Systems" column~~ to further define~~s~~ 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-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X~~7~~ Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-X~~7~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-X~~7~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X~~7~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-X~~7~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X~~7~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-X7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X~~7~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X~~7~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-X~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and ~~2.~~ PACS ~~3.~~2.	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter.

CIP-004-X~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-X~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-X~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-X~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-X~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to ~~for BES Cyber System Information~~BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable~~ility~~ Systems**	**Requirements**	**Measures**
6.1	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, ~~A~~authorize (unless already authorized according to Part 4.1.)~~provisioning of access to BCSI~~ based on need ~~(unless already authorized according to Part 4.1.)~~, as determined by the Responsible Entity, except for CIP Exceptional Circumstances~~:~~. 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2 Provisioned physical access to physical BCSI. Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).	Examples of evidence may include, but are not limited to, ~~the following:~~ individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access. • ~~Dated authorization records for provisioned access to BCSI based on need; or~~ • ~~List of authorized individuals~~

CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable~~ility~~ Systems**	**Requirements**	**Measures**
6.2	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an ~~Is~~ authorization~~ed~~ record; and 6.2.2. ~~Is~~ still need the provisioned access to perform their current work functions, ~~appropriate based on need,~~ as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; ~~and~~ • List of individuals who have been provisioned access; ~~and~~ • ~~List of privileges associated with the authorizations; and~~ • ~~List of privileges associated with the provisioned access; and~~ • ~~Dated documentation of the 15-calendar-month verification; and~~ • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-004-X~~7~~ Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable~~ility~~ Systems**	**Requirements**	**Measures**
6.3	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

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

- The 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 ~~Compliance Enforcement Authority~~ CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment Processes~~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-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				previous PRA completion date. (3.5)	the previous PRA completion date. (3.5)	for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has not implemented one or more documented program(s) for access management that includes a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action,	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and**	**Medium**	The Responsible Entity has implemented one or more progam(s) as	The Responsible Entity has implemented one or more program(s) as	The Responsible Entity has implemented one or more program(s) as	The Responsible Entity did not implement one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~7~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations Planning		required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do	required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use	required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more process(es) to remove the individual's ability to	access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more process(es) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			so by the timeframe required in Requirement R6, Part 6.3. The Responsible Entity has implemented one or more documented access management program(s) for BCSI but did not implement one of the applicable items for Parts 6.1 through 6.3. (R6)	provisioned access to BCSI but, for two individuals, did not do so by timeframe required in Requirement R6, Part 6.3. The Responsible Entiy implemented one or more documented access management program(s) for BCSI but did not implement two of the applicable items for Parts 6.1 through 6.3 (R6)	use provisioned access to BCSI but, for three individuals, did not do so by timeframe required in Requirement R6, Part 6.3. The Responsible Entity implemented one or more documented access management program(s) for BCSI but did not implement three of the applicable items for Parts 6.1 through 6.3 (R6)	The Responsible Entity has implemented one or more process(es) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by timeframe required in Requirement R6, Part 6.3. The Responsible Entity did not implement one or more documented access management program(s) for BCSI (R6)

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to

Version	Date	Action	Change Tracking
			revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
10-day final ballot	May 2021
Board adoption	November 2021

A. Introduction

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

2. **Number:** CIP-004-X~~6~~

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~Special Protection System (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**~~

4.1.6.4.1.5. Reliability Coordinator

4.1.7.4.1.6. Transmission Operator

4.1.8.4.1.7. 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 ~~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-004-X6:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-004-X6.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-X~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-X~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-X6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-X6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-X6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-X6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-X6 Table R4 — Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 0. EACMS; and 0. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 0. A dated listing of authorizations for BES Cyber System information; 0. Any privileges associated with the authorizations; and 0. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-X6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-X6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS; and~~ ~~PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~EACMS; and~~ ~~PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.~~	~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.~~
5.3~~4~~	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 5.1 ~~or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-X6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.45	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI. Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

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, 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 the NERC Reliability Standards in their respective jurisdictions.

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 Eapplicable 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 EThe applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible EThe 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 EnforceAssessment Programcesses:

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.

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-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information~~	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented~~	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is~~	access~~,~~ or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			storage locations, privileges were incorrect or unnecessary. (4.4)	processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Same Day Operations and Operations Planning	Medium	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~ ~~OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4~~2~~3) OR The Responsible Entity has implemented one or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access~~,~~ or unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4~~5~~) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the	reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar~~	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances. (5.54)	day following the effective date and time of the termination action. (5.3)		
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

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

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

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

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

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

Requirement R2:

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this~~

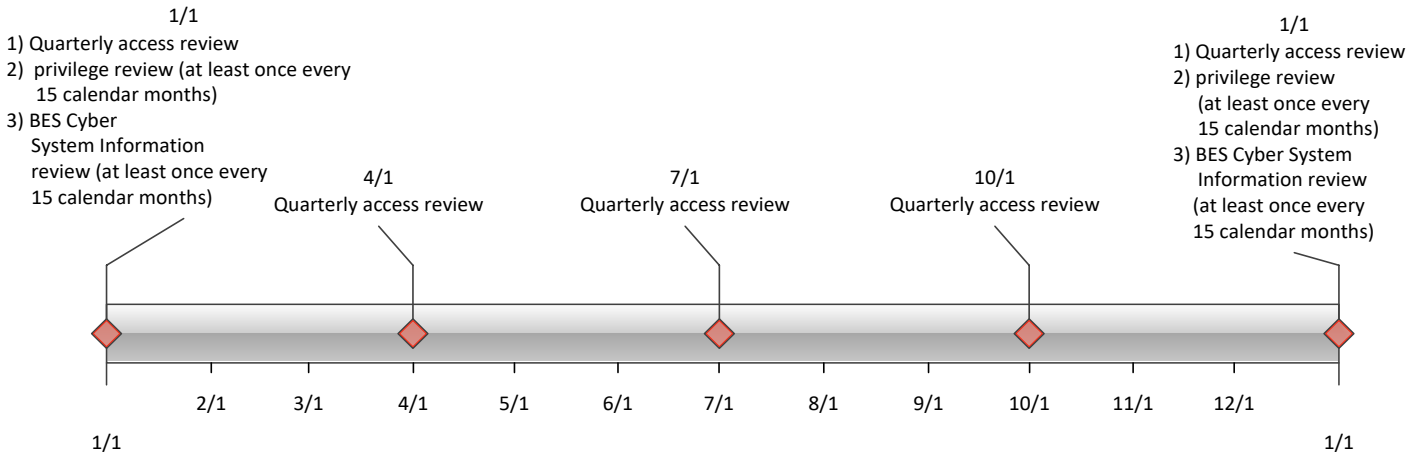
~~could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.~~

~~Requirement R4:~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

~~Rationale:~~

~~During 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:~~

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

~~Rationale for Requirement R2:~~

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

~~Rationale for Requirement R3:~~

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

~~Rationale for Requirement R4:~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.~~

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

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
10-day final ballot	May 2021
Board adoption	November 2021

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-X

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-X:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-X.

6. Background:

Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS		• Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "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 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 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 applicable 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:

- The 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity implemented one or more documented processes but did not include disposal or	The Responsible Entity has not documented or implemented any processes for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	applicable requirement parts in CIP-011-X Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
~~45-day formal or informal comment period with ballot~~	~~August 2020~~
10-day final ballot	~~September~~ May 2021~~0~~
Board adoption	November 2021~~0~~

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-X~~3~~

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-X~~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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-X~~3~~.

6. Background:

Standard CIP-011 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" ~~and "Applicability"~~ Columns in Tables:
Each table has an "Applicable Systems" ~~or "Applicability" column. The "Applicable Systems"~~ column to further define~~s~~ 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-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X~~3~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X~~3~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X~~3~~ Table R1 – Information Protection Program			
Part	**Applicable Systems~~ility~~**	**Requirements**	**Measures**
1.1	~~BCSI pertaining to:~~ High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	~~BCSI as identified in Part 1.1~~High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use; or

	1. EACMS; and 2. PACS		• Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements). • ~~Evidence of methods used to protect and securely handle BCSI during its lifecycle, including:~~ • ~~Electronic mechanisms,~~ • ~~Physical mechanisms,~~

CIP-011-X~~3~~ Table R1 – Information Protection Program			
Part	**Applicable Systems~~ility~~**	**Requirements**	**Measures**
			• ~~Technical mechanisms, or~~ • ~~Administrative mechanisms~~

CIP-011-X3 Table R1 — Information Protection Program			
Part	Applicability	Requirement	Measure
1.3	BCSI as identified in Part 1.1	When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement risk identification and assessment method(s) for the following: 1.3.1 Data governance and rights management; and 1.3.2 Identity and access management; and 1.3.3 Security management; and 1.3.4 Application, infrastructure, and network security.	Examples of acceptable evidence may include, but are not limited to, dated documentation of the following: • Implementation of the risk identification and assessment method(s) (1.3); • Vendor certification(s) or Registered Entity verification of vendor controls implemented from the under-layer to the service provider, including application, infrastructure, and network security controls as well as physical access controls (1.3.2, 1.3.3, 1.3.4); • Business agreements that include communication expectations and protocols for disclosures of known vulnerabilities, access breaches, incident response, transparency regarding licensing, data ownership, and metadata (1.3.1); • Consideration made for data sovereignty, if any (1.3.1);

			• ~~Considerations used to assess conversion of data from one form to another and how information is protected from creation to disposal (1.3.1, 1.3.3);~~ • ~~Dated documentation of vendor's identity and access management program (1.3.2); and~~ • ~~Physical and electronic security management documentation, (e.g., plans, diagrams) (1.3.3).~~
~~1.4~~	~~BCSI as identified in Part 1.1~~	~~When the Responsible Entity engages vendor services to store, utilize, or analyze BCSI, implement one or more documented electronic technical mechanisms to protect BCSI.~~	~~Examples of evidence may include, but are not limited to, dated documentation of the following:~~ • ~~Description of the electronic technical mechanism(s) (e.g., data masking, encryption, hashing, tokenization, cypher, electronic key management method[s]);~~ • ~~Evidence of implementation (e.g., configuration files, command output, architecture documents); and~~ • ~~Technical mechanism(s) for the separation of duties, demonstrating that entity's control(s) cannot be subverted by the custodial vendor.~~

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-X~~3~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI~~BES Cyber Information~~ prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

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

- The 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 Compliance Enforcement AuthorityCEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment ProcessesEnforcement 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.

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A ~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the applicable items for Parts 1.1 through 1.4. (R1)~~	N/A ~~The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the applicable items for Parts 1.1 through 1.4. (R1)~~	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2) ~~The Responsible Entity implemented one or more~~	The Responsible Entity neither documented nor implemented ~~did not implement~~ one or more BCSI ~~documented information~~ protection program(s). (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X~~3~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~documented information protection program(s) but did not implement three or more of the applicable items for Parts 1.1 through 1.4. (R1)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-X~~3~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021

Anticipated Actions	Date
10-day final ballot	May 2021
Board adoption	November 2021

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-X~~2~~

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-X~~2~~:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-X~~2~~.

6. Background:

Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X~~2~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X~~2~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X~~2~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify ~~information that meets the definition of BES Cyber sytem Information~~ BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify ~~BES Cyber System Information~~ BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~ BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify ~~BES Cyber System Information~~ BCSI; or • ~~Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.~~ • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-~~2~~X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	~~Procedure(s) for protecting and~~Method(s) to protect and securely handl~~e~~ing ~~BES Cyber System Information~~BCSI~~, including storage, transit, and use~~to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use ~~of BES Cyber System information~~; or • Records indicating that ~~BES Cyber System Information~~ BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical

CIP-011-X~~2~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain ~~BES Cyber System Information~~ BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyebr System Information~~ BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain ~~BES Cyber System Information~~BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~ BCSI prior to the disposal of an applicable Cyber Asset.

B. 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, 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 ~~the NERC~~ 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 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 applicable 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~~.~~:

~~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~~ The applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~Responsible~~ applicable ~~E~~entity is found non-compliant, it shall keep information related to the noncompliance 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 Process~~ 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2) ~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented ~~a~~ one or more ~~BES Cyber System Information~~ BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X~~2~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.1)	include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-X~~2~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

~~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:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~**Requirement R2:**~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

~~quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.~~

~~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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Rationale for Requirement R2:~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of Project 2019-02 BES Cyber System Information (BCSI) Access Management is to clarify the CIP requirements related to both managing access and securing BCSI. This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

[1] See subject standards for additional information on Distribution Providers subject to the standards.

General Considerations

The 24-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011; and
- Administrative overhead to review their program.

The 24-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide Electric Reliability Organization (ERO) and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-X – Cyber Security - Personnel & Training

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 twenty-four (24) 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 twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-X – Cyber Security - Information Protection

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 twenty-four (24) 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 twenty-four (24) 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

Responsible Entities shall initially comply with the periodic requirements in the CIP-004-X and CIP-011-X within the periodic timeframes of their last performance under the CIP-004-6 and CIP-011-2.

Compliance Dates for Early Adoption of Revised CIP Standards

A Responsible Entity may elect to comply with the requirements in CIP-004-X and CIP-011-X following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-X and CIP-011-X Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-X in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-02 BES Cyber System Information Access Management** by **8 p.m. Eastern, Monday, May 10, 2021.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

Background Information

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Questions

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?
   - ☐ Yes
   - ☐ No

   Comments:

9. Please provide any additional comments for the SDT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

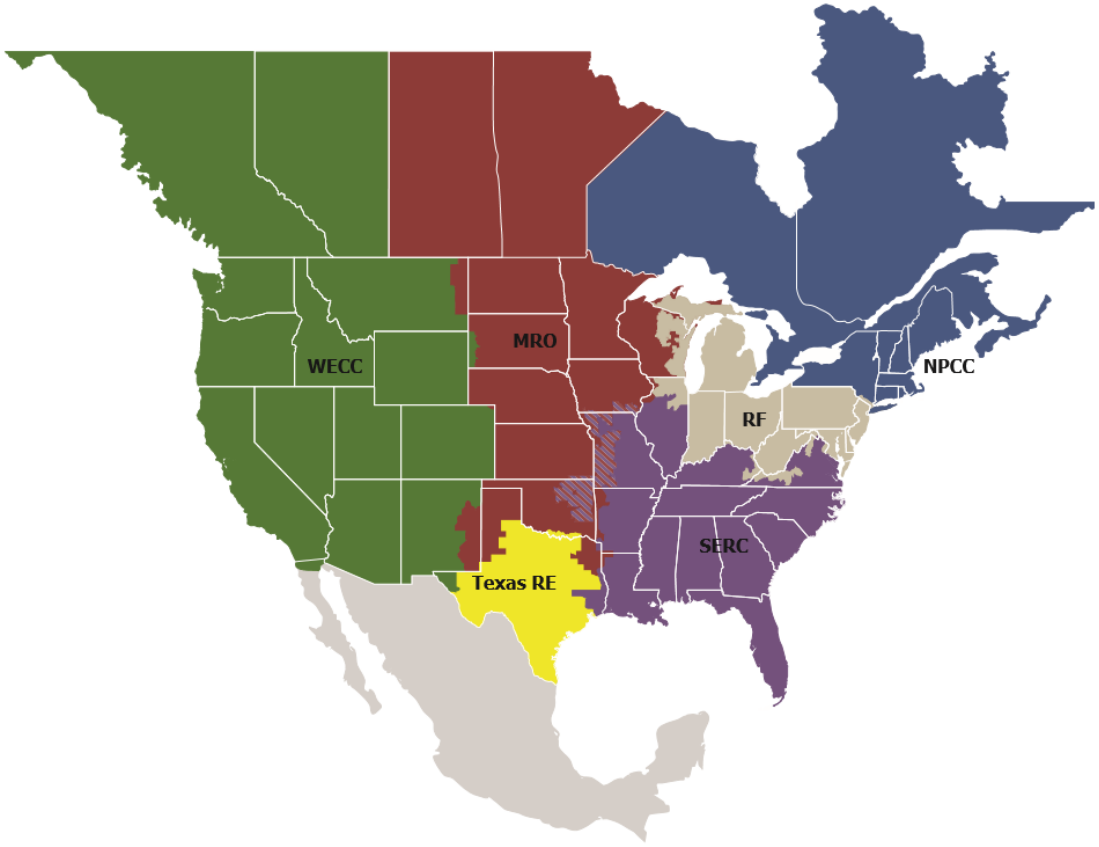
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the intent of the Standard Drafting Team (SDT) in drafting the requirements. This Technical Rationale and Justification for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving and initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT modified Reliability Standard CIP-004-X to require Responsible Entities to implement specific controls in Requirement R6 to authorize, verify, and revoke provisioned access to BES Cyber System Information (BCSI).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1

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

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

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

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

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

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

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

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals' ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have

changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.

Attachment 1: Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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

Requirement R2:
Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber

security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

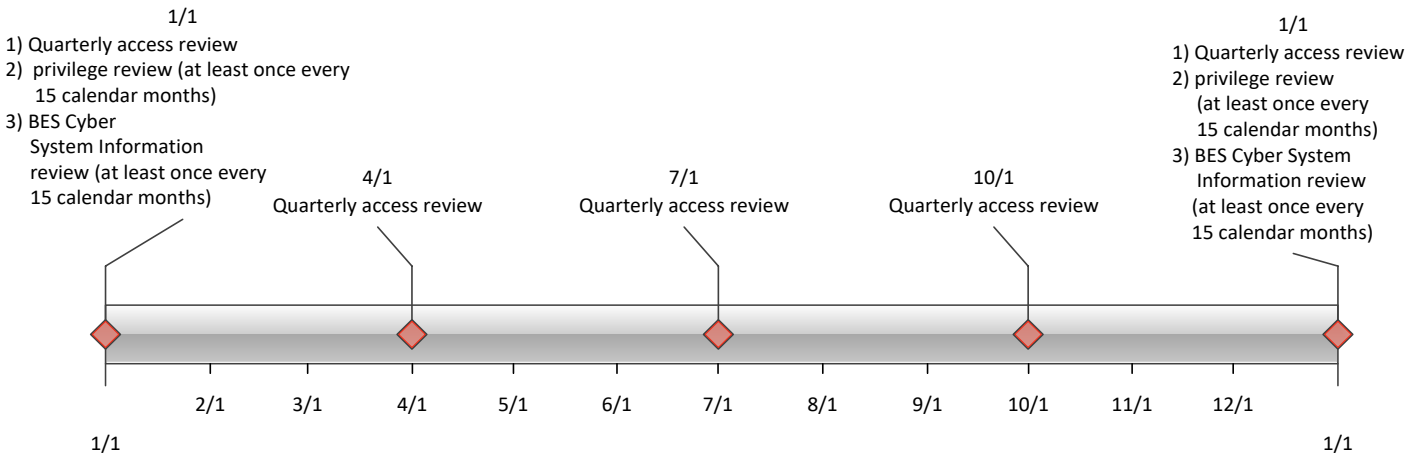
There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:
Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

An example timeline of all the reviews in Requirement R4 is included below.



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

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

Requirement R5:
The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

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

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

following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

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

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

Rationale for Requirement R5:
The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

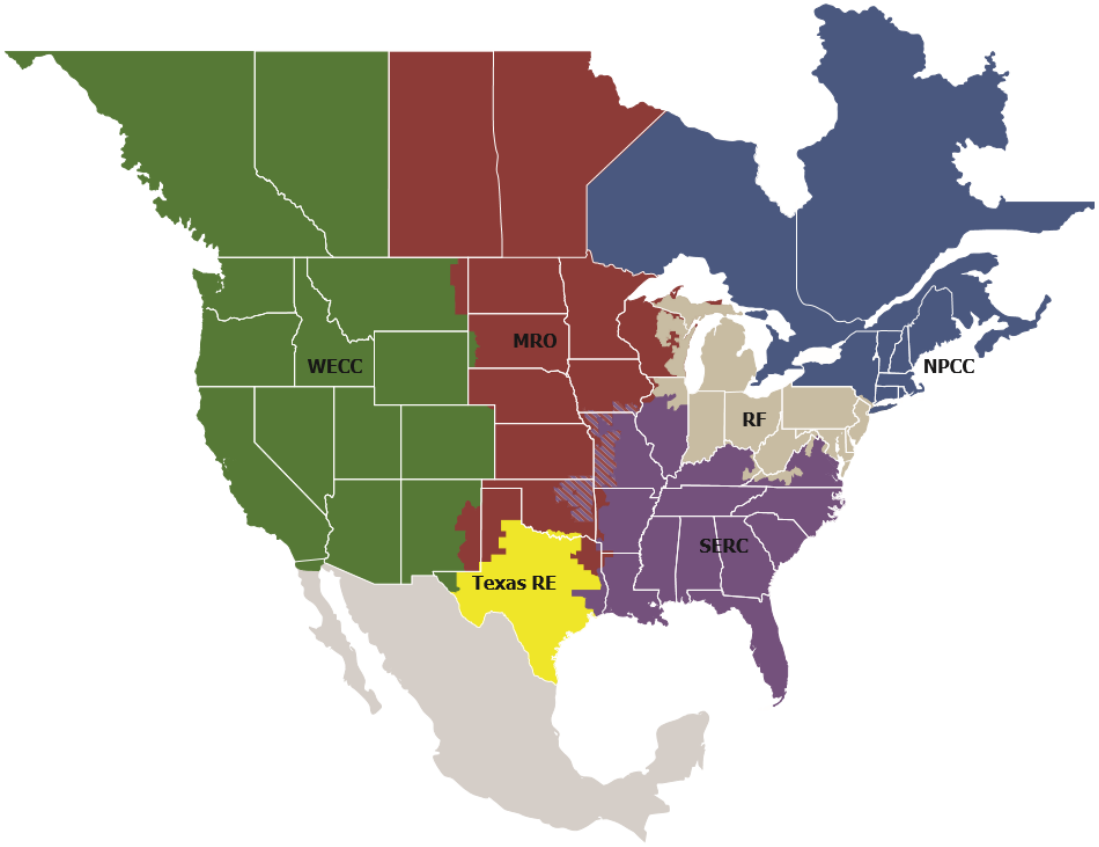
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-011-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving an initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI), by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-011-X to require Responsible Entities to implement specific methods in Requirement R1 for administrative, technical, and physical controls related to BCSI during storage, handling and use including when utilizing vendor provided cloud services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Modifications to Requirement R1:

Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1

Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Attachment 1: Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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:

Responsible Entities are free to utilize existing change management and asset management systems.
However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information. Requirement R1 Part 1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in Requirement R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal. The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.
>
> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CDRW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 of Trustees approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Implementation Guidance for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

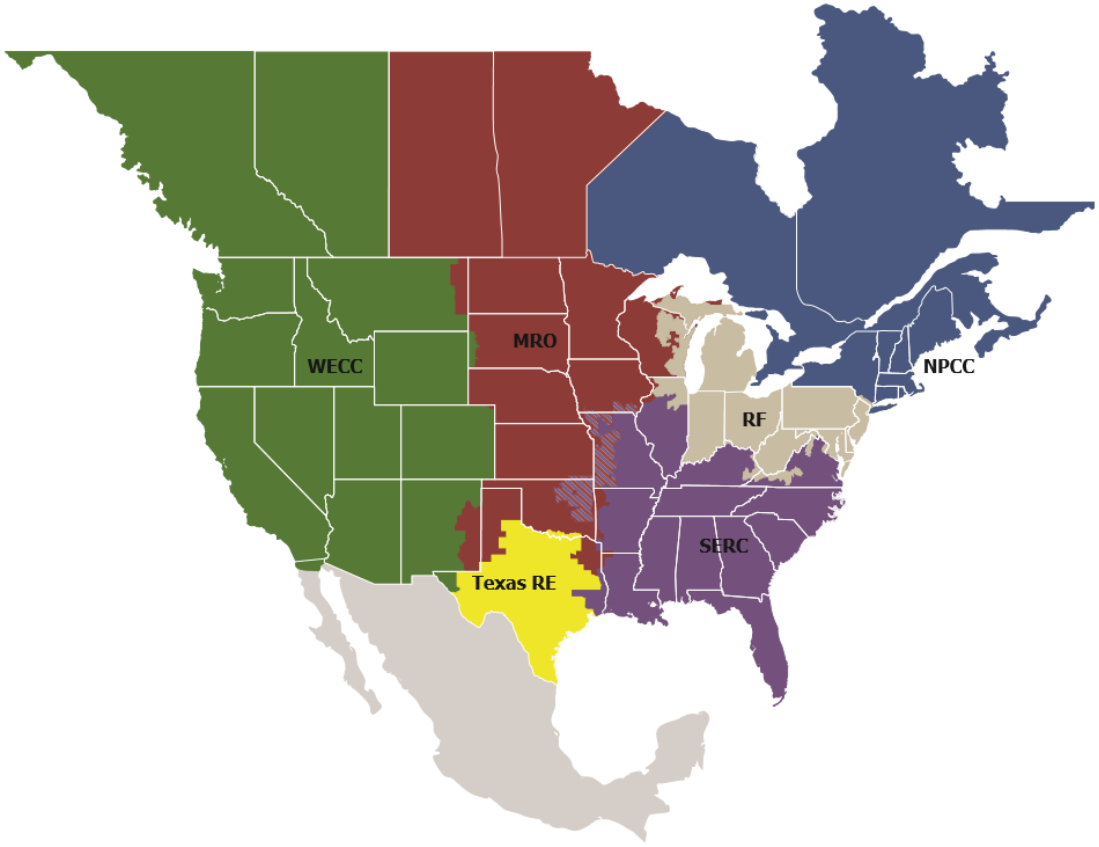
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-004-X. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for the modifications to CIP-004-X.

[1] NERC's Compliance Guidance Policy

Requirement R1

General Considerations for Requirement R1

None

Implementation Guidance for R1

None

Requirement R2

General Considerations for Requirement R2

None

Implementation Guidance for R2

The Responsible Entity has the flexibility to define the training program, and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles, or responsibilities at the discretion of the Responsible Entity.

Requirement R3

General Considerations for Requirement R3

None

Implementation Guidance for R3

None

Requirement R4

General Considerations for Requirement R4

None

Implementation Guidance for R4

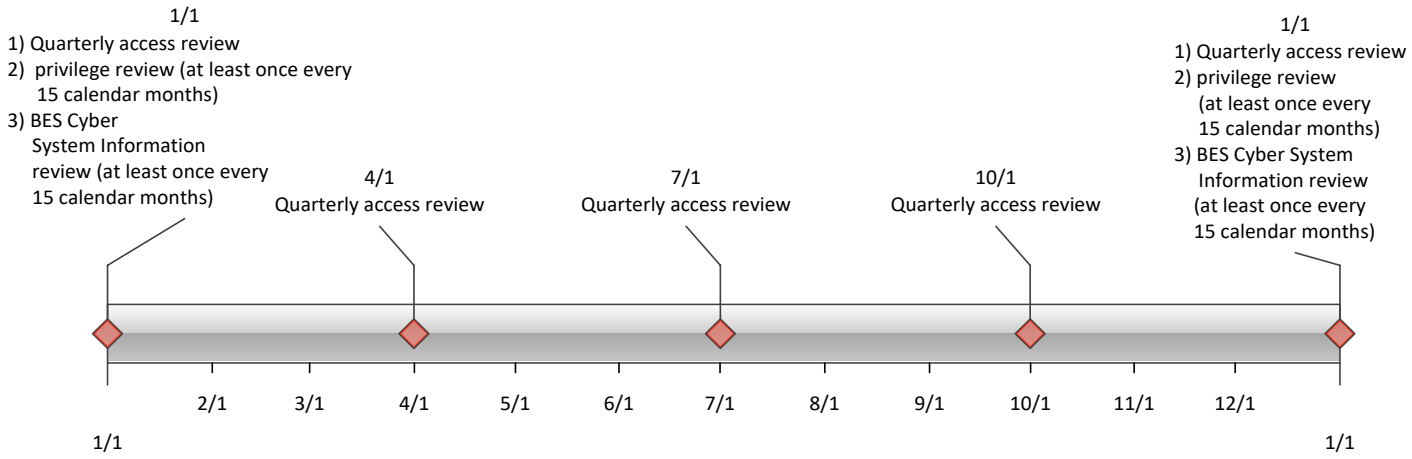
Consider including the person or persons empowered by the Responsible Entity to authorize access in the delegations referenced in CIP-003-8.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

Quarterly reviews can be achieved by comparing individuals actually provisioned access against records of individuals authorized for provisioned access. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

Entities can more efficiently perform the 15-calendar-month review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed.

An example timeline of all the reviews in Requirements R4 and R6 is included below.



Requirement R5

General Considerations for Requirement R5

None

Implementation Guidance for R5

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

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

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

If an entity considers transitioning a contracted individual to a direct hire, an entity should consider how they will meet the evidentiary requirements for Requirements R1 through R4. If evidence for compliance with Requirements R1 through R4 cannot be provided, the entity should consider invoking the applicable sub-requirements in Requirement R5 for this administrative transfer scenario. Entities should also consider including this scenario in their access management program, including a higher-level approval to minimize the instances to which this scenario would apply.

Requirement R6

General Considerations for Requirement R6

None

Implementation Guidance for R6

This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the 15-calendar-month verification in Requirement R6. The person reviewing should be different than the person provisioning access.

Entities may choose not to provision access, or provision temporary rather than persistent access, for authorized users. In other words, an authorized individual does not have to have any access provisioned, but all provisioned access must be authorized.

An entity can choose to give an authorization to access any BCSI, or they can have authorizations for specific storage locations or types of BCSI, if they so choose.

While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint

where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program. In this case, the review required in Requirement R6 Part 6.2 should still be performed, and the revocation required in Requirement R6 Part 6.3 could consist of removing the individual's name from the authorized list at the time of termination or upon review when it is determined the individual no longer has a need.

Entities can more efficiently perform the 15-calendar-month BCSI review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. For an example timeline to perform the 15-calendar-month BCSI review, refer to the graphic in the *Implementation Guidance for R4* section.

An example where a termination action in Requirement R5 Part 5.1, satisfies Requirement R6 Part 6.3, would be the Responsible Entity revoking an individual's means of unescorted physical access and Interactive Remote Access (e.g., physical access card, virtual private network, Active Directory user account). By revoking both physical and electronic access, the individual could ultimately not have access to BES Cyber System Information. The Responsible Entity should still revoke access that is manually provisioned (e.g., local user account, relay, site area network server, cloud based BCSI that is not tied to an active directory account).

Appendix 1: Implementation Guidance for CIP-004-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale sencan be found in a separate Technical Rational document for this standard.

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

Requirement R1:
Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:
The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Requirement R3:
Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check.

Requirement R4:
To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The list of provisioned individuals can be an automatically generated

account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

Requirement R5:
Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-X. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-X, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-X, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R5
The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R5
The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-X, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-X R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

VSL Justifications for CIP-004-X R6	
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 requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby 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 VSLs are based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-X. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-X, Requirement R1

The VSL justification is below.

VSLs for CIP-011-X, R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)

VSL Justifications for CIP-011-X, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed revisions do not lower 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 VSLs are 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 VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented information protection program(s) that collectively include the applicable requirement parts in CIP-011-X Table R1 – Information Protection Program.

VRF Justification for CIP-011-X Requirement R2

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-X Requirement R2

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 and R5 to CIP-004-X R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	CIP-004-X, Requirement R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes clarification on the specific elements within an access management program that need to be implemented. In addition, a definition of what constitutes BCSI access was included in the parent R6 requirement language.
CIP-004-6, Requirement R4, Part 4.1.3	**CIP-004-X, Requirement R6, Part 6.1, 6.1.1, and 6.1.2**	The modified requirement language includes a shift from authorizing access to designated

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI. Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).	storage locations, to authorizing the provisioned access to BCSI. The Note was included to specify the type of access to be authorized (6.1), verified (6.2) and revoked (6.3).
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	**CIP-004-X, Requirement R6, Part 6.2, 6.2.1, and 6.2.2.** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is still needed.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R5, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	**CIP-004-X, Requirement R6, Part 6.3** For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.
CIP-004-6, Requirement R5, Part 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**CIP-004-6, Requirement R5, Part 5.3** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	This Part was renumbed from 5.4 to 5.3 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. The reference within the Part was changed to just Part 5.1.
CIP-004-6, Requirement R5, Part 5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the	**CIP-004-6, Requirement R5, Part 5.4** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating	This Part was renumbed from 5.5 to 5.4 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. This is a renumbering change only, no changes were made to the Part's requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-X

The modifications made to requirements within CIP-011-X are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use).

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection Program*.	**CIP-011-X, Requirement R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to Applicable Systems that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program.*	Parent CIP-011-X Requirement R1 language modified to sharpen focus on protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems, which may contain BCSI.
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	**CIP-011-X, Requirement R1, Part 1.1** Method(s) to identify BCSI.	Requirement language simplified.

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	**CIP-011-X, Requirement R1, Part 1.2** Method(s) to protect and securely handle BCSI to mitigate the risks of compromising confidentiality.	Requirement revised to broaden the focus around the implementation of controls that mitigate the risks of compromising confidentiality in any state, not just storage, transit, and use.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through May 10, 2021

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, May 10, 2021** for the following:

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection
- Implementation Plan

Due to projects 2019-02 BES Cyber System Information Access Management (BCSI) and 2016-02 Modification to CIP Standards (2016-02) both modifying CIP-004 and CIP-011, an "-X" has been added in place of the version numbers for BCSI and a "-Y" for the 2016-02 standards. Once both projects are completed, they will be combined together with one version, prior to submission to the NERC Board.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted April 30 – May 10, 2021.

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

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-02 BCSI Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

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:	2019-02 BES Cyber System Information Access Management (Draft 3)
Comment Period Start Date:	3/25/2021
Comment Period End Date:	5/10/2021
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 AB 3 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 3 ST 2019-02 BES Cyber System Information Access Management Implementation Plan AB 3 OT

There were 64 sets of responses, including comments from approximately 157 different people from approximately 98 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?

9. Please 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
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	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
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC

					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO,WECC	Southwest Power Pool Standards Review Group (SSRG)	Kim Van Brimer	SPP	2	MRO
					Jim Williams	SPP	2	MRO
					Matt Harward	SPP	2	MRO

					Shannon Mickens	SPP	2	MRO
					Alan Wahlstrom	SPP	2	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC

					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen	5	NPCC

	Engineered Solutions International Inc.		
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC

					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
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
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma	1	MRO

						Gas and Electric Co.		
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The use of provisioned access is not addressed in CIP-004-X Requirement 5. The CIP-004-X requirements should use consistent terminology.	
Likes 0	
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	2019-02_Unofficial_Comment_Form_03252021_Information-Protection-NSRF-draft-1_JC.docx
Comment	

Comments: WAPA believes the SDT is moving in the correct direction from the past version. WAPA does not support the term "provisioned access" as it is a non-definable term which has the potential to confuse regulators (auditors, risk, enforcement, FERC, NERC, etc…) and industry. The term also does not address the requirements in the SAR for entities storing BCSI off-prem (such as cloud data centers).

"Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas "access to BCSI" occurs when an individual has both "the ability to obtain and use BCSI," we recommend changing "provisioned access" to "access" that ensures only authorized individual can possess BCSI.

The use of "provisioned, provision or provisioning" of "access," regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the "provisioned" configurations of entity BES Cyber System Information repositories in order to "verify" the "authorization" of such provisioned access.

The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers may not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI without litigation, yet entities will be asked to provide this information for an entire audit cycle

Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 " to prevent unauthorized access to BES Cyber System Information." This allows entities to determine the risk and methods to protect BCSI

4. WAPA recommends addressing the two potential controls for access to off-prem BCS, 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. This could be as simple as:

Implement at least one control to authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

In AEP's opinion, the updated language leaves room for interpretation. It might be simplistic to refer to the subparts of R6 instead of using specific words from the subparts.

The updated Requirement 6 would read: "Each Responsible Entity shall implement one or more documented access management program(s) to *meet subparts of R6 for provisioned access* to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP- 004- X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]."*

Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	

We disagree with "provisioned access" since there is a security concern where it only requires authorization for a provisioned access. If an access to BCSI is not provisioned, it means no authorization is required. This doesn't meet the goal of SAR for controlling access to BCSI. Given that R6 has defined "access to BCSI" as an individual has both the ability to obtain and use BCSI, we suggest changing "provisioned access" to "access" that ensures only authorized individual can possess the BCSI. Also "unless already authorized according to Part 4.1" should be removed as having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.

Recommendations:

We have the following suggested language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Providing the definition of “provisioned access” within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for “Provisioned Access.”

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	No
Document Name	

Comment

•"Prior to provisioning, authorize **provisioned** access"? Wouldn't it be more appropriate to remove "provisioned" in 6.1.1 and 6.1.2? How can an entity authorize provisioned access if it hasn't been provisioned yet?

• R6 requires provisioned access to BCSI to be authorized based on need, reviewed, and revoked upon a termination action.

• R6 makes no mention of “Transfers or reassignments”. R5 does not address revoking provisioned access to BCSI either, therefore entities are not required to revoke provisioned access to BCSI unless they are terminated.

• Provisioned access to BCSI does not require an individual to have Cyber Security Awareness training or a PRA. Could an individual have no access to a BCS but have all of the information relating to the BCS.

•In the Note section of R6.1 “Provisioned access is to be considered the result of the specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).”

{C}- Recommend changing the e.g., section to read “physical keys or access control key cards, user accounts and associated rights and privileges, encryption keys).

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While the SDT did well in clarifying the intent of the provisioning, we do not feel a “Note” inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
While the SDT did well in clarifying the intent of the provisioning, we do not feel a “Note” inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	2019-02_Unofficial_Comment_Form_Final Draft.docx

Comment

For the purposes of providing for cloud storage and processing of BCSI information, the proposed changes are sufficient to provide for its use. However, the changes are silent with regard to the authorized incidental access of BCSI in a physical environment such as a meeting. It is recommended that clarification be provided in the requirement language for such circumstances. This is addressed in the Technical Rationale: however, it was not included in the standard.

The following modification is suggested to the Note in requirement part 6.1:

Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	

Comment

Part 6.1 perhaps should read as follows:

Unless already authorized according to Part 4.1, authorize provisioned access based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 1,3,5,6

Answer	No
Document Name	

Comment

The term “provisioned access” adds another undefined term to the NERC standards and doesn’t provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.

a. “Provisioned access” creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas “access to BCSI” occurs when an individual has both “the ability to obtain and use BCSI,” we recommend changing “provisioned access” to “access to BCSI”.

b. The term “unless already authorized according to Part 4.1” should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.

c. The use of “provisioned, provision or provisioning” of “access,” regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the “provisioned” configurations of entity BES Cyber System Information repositories in order to “verify” the “authorization” of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle

d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3rd party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)

Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.

2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 “ to prevent unauthorized access to BES Cyber System Information.” This allows entities to determine the risk and methods to protect BCSI

4. Consider using “authentication systems or encryption of BCSI” for personnel accessing electronic BCSI on cloud prem providers locations

Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST notes that words can only be nouns, verbs, adjectives, etc. on an individual basis. Calling any two-word phrase a noun is grammatically incorrect. Beyond that, the phrase, “provisioned access,” as used in proposed CIP-004 requirements, is itself grammatically incorrect by virtue of the fact “provisioned” is the past tense of the verb, “provision.” It is not an adjective. An individual can be given access or can be provisioned access but cannot be given provisioned access. Since the SDT has adopted NERC’s informal definition of “access to BCSI” as the ability to “obtain and use” it, N&ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI (or BCSI storage locations), dropping the misunderstood and grammatically incorrect “provisioned access.”	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed change to “provisioned access” and that the entity will determine how that provisioning will occur.	
Likes 0	

Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA and Indiana Comments	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC agrees that this change provides greater clarity regarding the intent of this requirement and understands that it is the provisioned access that must be authorized, verified, and revoked.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	EEI Near Final Draft Comments_ Project 2019-02_Rev_0f_For Review FOR MEMBER REVIEW.docx
Comment	
OG&E agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Assuming that “provisioned access” means when someone gains and keeps BCSI access? Meaning if someone sees (screen sharing in view mode only) does not fall under “provisioned access”?	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the proposed modifications. PG&E will define what is “provisioning of access” for our environment and will not need a defined NERC term since a NERC term may not cover all possible conditions for PG&E.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	

David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with the proposed change. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.	
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	
Southern agrees as with EEI that the change provides greater clarity regarding the intent of the Requirement.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes

Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Be careful adding “NOTES” to requirements. If the purpose is to increase clarity, then consider re-writing the requirement to improve clarify. NOTES may become overused across CIP standards and cause confusion.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	

IESO supports the comments submitted by NPCC.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

We support these changes.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) agrees that “provisioned access” is an improvement and supports the proposed change.

Likes 0	
Dislikes 0	

Response

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer

Answer	Yes
Document Name	

Comment

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy agrees that this change provides greater clarity regarding the intent of this Requirement.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	

Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The ISO/RTO Council Standards Review Committee (IRC SRC) acknowledges the SDT for addressing our prior concerns surrounding the lack of clarity associated with “provision of access.”	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PAC requests the SDT provide better definition of “provisioned access” than what was currently provided in Part 6.1	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that this change provides greater clarity regarding the intent of this Requirement. However, use of the term “note” creates ambiguity because it is not clear whether the language in the note creates mandatory obligations. The use of the word “note” should be removed and the language contained in the note in Requirement R6, Part 6.1 should be elevated to the parent Requirement R6 because the term “provisioned access” is used in other parts of Requirement R6. Additionally, the note language should be strengthened for additional clarity (e.g., “is to be considered” may not be clear for industry to understand what the note means)	
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	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Northern California Power Agency - 3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
disregard	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE seeks clarification regarding the scope of the revised CIP-004, Part 6.1. Specifically, Texas RE interprets “provisioned access” to include all instances in which an individual is “provisioned access” to BCSI. Accordingly, accidental or mistaken provisioned access would be within the scope of the requirement. Conversely, compromise of BCSI without any specific entity actions to provide the means to access BCSI (such as a data breach) would not be within the scope of the proposed requirement. Texas RE inquires as to whether this is the SDT’s intent.	
Likes 0	
Dislikes 0	
Response	
Doug Peterchuck - Omaha Public Power District - 1	
Answer	
Document Name	2019-02_Unofficial_Comment_Form_Information-Protection-OPPD.docx
Comment	
Likes 0	
Dislikes 0	
Response	

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment

Please provide additional clarification in the Standard, and in the technical rationale.

Does the term, 'use' allow a user to unencrypt? Potential here for resulting in a potential data manipulation.

Recommendation:

Only use the term, "access."

See the new R6 versus the former R4 language changes for clarification.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	

Comment

GRE agrees to adding "obtain and use" language to clarify what constitutes an access to BCSI, but disagree to the use of "provisioned access". After clarifying the access to BCSI, the language "provisioned" should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

Recommendations:

1. Only use the term "access" as recommended in Q1

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy suggests “obtain and use” be included within R6 statement. “Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access **that grants the ability to obtain and use** BCSI pertaining to the “Applicable Systems” identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
Additional clarity is needed for what constitutes access by “obtain and use”. Specifically, clarify what “use” means by defining the point at which information is considered “used”. Does “use” mean immediately when the information is read by someone, or does it mean when the information is applied for some purpose? For example, if someone obtains information and can read it, and there are additional physical or electronic controls in place to prevent unauthorized use of the obtained information, do those controls then prevent “access to BCSI” based on the premise that information must be obtained and used to constitute access to BCSI?	
Likes 0	
Dislikes 0	
Response	

Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	

Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	

Comment
Integrity should also be included as a security objective for BCSI in addition to confidentiality. Removing “obtain and use” is not consistent with the ERO Enterprise CMEP Practice Guide nor is it consistent with https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf In the R6 Requirement language "To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI." - This statement contradicts the Requirement of R6.1. If a user must concurrently have the ability to both, obtain and use BCSI how does that provide the entity the ability to authorize based on need, as determined by the Responsible Entity? - The webinar on 4/27/2021 attempted to clarify what the right and left lateral limits of BCSI “use” could be, but further clarifications might be needed to ensure a consistent approach is expected for authorization and provisioning.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Access needs to be better defined, in particular the phrase “use BCSI” – being able to view a document or taking advantage of the information in the document. Is it “I have access to the file but not able to open it”, or is it “I have BES cyber system IP address, but no ability to get to those systems because there are other controls preventing me from using that information”? Where is it in the standard that this is spelled out as a clear definition – “two-prong test”? This is not clear in the question above – shouldn’t the requirement be more clear?

Likes 0	

Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	

Comment
The placement of the “obtain and use” statement gets lost within the construct of the Requirement Language, it appears as an add-on to the high level R6 language. Suggested alternative: “Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke the provisioned access that grants the ability to obtain and use BCSI pertaining to the “Applicable Systems” identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-X Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]”

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment
We agree to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw (See our comments in Q1).

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
Dominion Energy is of the opinion that the terms“obtain and use” are ambiguous. We suggest additional language that provides for the Registered Entity to have the felxibility to define how these terms are applied by adding some additional language to the proposed Requirement as follows: …*an individual has both the ability to obtain and use BCSI as defined by the Registered Entity.*

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment
1. We agree to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to the use of “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1). **Recommendations:** 1. Only use the term “access” as recommended in Q1

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
A user can have provisioned access to obtain BCSI and not use it. The Registered Entity is currently receiving an authorization for a user based on need to access BCSI. Access to BCSI is enough to constitute an authorization regardless of use. While this clarification assists in the context of third-party solutions it does not provide clarity for electronic or physical access to BCSI.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the clarifying language contained in the two-prong test (i.e., “obtain and use”) provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. EEI also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.	
Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills would recommend that 6.1’s “Note” section use the same language as R6 opening paragraph. Specifically “ability to obtain and use” should be used whenever possible, in this instance the “Note” section may read like this, “Provisioned access is to be considered the result of the specific actions resulting in an individual’s ability to obtain and use BCSI.”	
Likes 0	

Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the reinstatement of “obtain and use” concepts.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NVE agrees that the clarifying language contained in the two-prong test (i.e., "obtain and use") provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. NVE also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees that the two-pronged test is an improvement over the existing language. Texas RE is concerned, however, that the verbiage “obtain and use” is subject to further interpretation. One approach could be to clarify the verbiage to read: “*the authorized ability to retrieve, modify, copy, or move BCSI*”. Alternatively, Texas RE recommends creating bright line criteria establishing what it means for the BCSI to be usable.	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
The ‘obtain and use’ language introduced provides valuable clarification with regard to provisioning and deprovisioning of access and provides context that will enable clearly defined opportunities to leverage cloud services. However, as drafted, the standard effectively provides different explanations for "access” versus “provisioned access.” It would increase clarity if these explanations were combined. It is recommended that the note explaining provisioned access be moved to the main requirement so that all explanatory statements regarding access or provisioned access are in the same place. In this manner, it is clear that the clarifications to “provisioned access” apply across all parts of requirement R6. Consistent with our recommendation to question 1 regarding incidental access, this would modify the main requirement of R6 as follows: …To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles etc.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	

Comment
Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	

Comment
Entergy supports the inclusion of the "obtain and use" language from the CMEP Practice Guide. This language clarifies that users with "access" for purposes of the requirement must be able to obtain and use BCSI, which addresses industry's concern regarding encrypted data. In particular, the prior language could present a grey area where a user could receive an encrypted BCSI item and be considered as having the BCSI even though they (conceivably) could not use it. This approach aligns with Entergy's interpretation under both its current BCSI program, as well as the guidance and position we are pursuing for BCSI in the cloud

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	

Comment
AEPC has signed on to ACES 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 NPCC Regional Standards Committee	
Answer	Yes
Document Name	

Comment	
We support the update to this Requirement language.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Support the update to this Requirement language.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this update.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.

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

Southern agrees that for access to occur, a user must both obtain BCSI and possess the ability to use BCSI according to the CMEP dated April 26, 2019.

Likes 0	
Dislikes 0	

Response

David Hathaway - WEC Energy Group, Inc. - 6

Answer	Yes
Document Name	

Comment

Support comments made by EEI.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

We support EEI comments.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E agrees that the clarification is sufficient.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	Yes
Document Name	

Comment

OKGE supports comments provided by EEI.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

AEP agrees with the addition of “obtain and use” language in R6 parent requirement, as this is in alignment with AEP’s BCSInfo program.

Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
The SPP Standards Review Group (SSRG) recommends the word “use” have clarity supplied around the term.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC appreciates the SDT’s efforts to include the concept from the CMEP Practice Guide. However, we would prefer the language be more specific to CIP-004, rather than re-introduce the broader “access” concept that goes beyond CIP-004 by using this language instead: “An individual is considered to have provisioned access to BCSI if they concurrently have the means to both obtain and use the BCSI (e.g., an individual who obtains encrypted BCSI but does not have the encryption keys does not have provisioned access).” The example is helpful in understanding what is meant by “obtain and use.”	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA Contents.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	

Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees the proposed changes make it clear that both parameters of the two-pronged test for “obtain and use” must be met to constitute “access” to BCSI.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Storage locations identified for using BCSI is reference in CIP-011-X. CIP-004-X and CIP-011-X should provide consistent terminology.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

1.

i. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1).

ii. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No

Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, “Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.” Removing “storage locations” from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence. Similar to “Provisioned access” noun, simply stating “BCSI” will make it intangible where keeping “storage locations” will make the requirement and its subparts tangible.

AEP understands the intent but it is not clear based on how it is currently worded. AEP requests SDT to provide further clarification on the intent and to provide better definition on “provisioned access” than what was currently provided in Part 6.1 (“Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).)” AEP also recommends SDT to focus on auditable methods to protect BCSI at 3rd party off-premise (cloud) locations.

AEP currently defines what constitutes as storage locations in CIP-011-2 R1 information protection program, but for other smaller entities this may become further complicated to define besides managing access to BCSI storage locations.

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

To ensure a consistent understanding of the issues surrounding information storage on the cloud, Dominion Energy suggests using language similiar to that in CIP-011 that addresses cloud storage in the proposed CIP-004.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1). The objective of SAR and NERC CMEP BCSI guidance is to prevent unauthorized access to BCSI rather than “provisioned access to BCSI”. Using “provisioned access to BCSI is lowing the bar for the BCSI authorization doesn’t meet the goal of SAR for controlling unauthorized access to BCSI. Also “provisioned access” is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider’s solution would likely be considered an EACMS based on the current EACMS definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case. Additionally many modern cybersecurity tools such as local endpoint protection systems, now make use of Cloud services to provide additional context to the information seen on local systems, and require that much of the system log data be pushed to the Cloud to enable this analysis.

Tacoma Power suggests modification of the EACMS definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using “provisioned access” based on our concerns in Q5.	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using “provisioned access” based on our concerns in Q5. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	

Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NVE agrees that the approach provides entities with the additional flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term “storage locations” does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities’ access management programs. Such guidance would be helpful to ensure backward compatibility.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	

a. GRE agrees to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1).

b. The requirement to provide lists of personnel with “provisioned access” would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	No
Document Name	
Comment	

The IRC SRC is concerned that keeping “storage locations” without defining it in the standard or the NERC Glossary will require entities to define it for themselves. This will create a variety of interpretations throughout the regions.

The IRC SRC recommends the SDT consider defining the term “storage locations” to indicate that storage locations may be physical locations or virtual locations that are protected using technologies such as access control or encryption

Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST strongly disagrees with the SDT's assertion that retention of "designated storage locations," is a hindrance to using third party / cloud services, and notes that the SAR for this project states the project will provide "…a secure path towards utilization of modern third-party data storage and analysis systems." The real roadblock here, for which solutions are already available, is encryption key management (see our response to Question 9). In addition, N&ST is concerned that one or more Regional Entities may or may not agree with the SDT's frequently repeated promise that managing access to BSCI storage locations will be accepted as a fully compliant equivalent to managing access to BCSI, and that Responsible Entities have the option of maintaining current practices. As a compromise, N&ST recommends the proposed CIP-004 changes be amended to state explicitly that Responsible Entities must manage access to one or more of: BCSI, designated electronic storage locations, and designated physical storage locations. This change would give entities the flexibility of maintaining or dropping "storage locations" or perhaps implementing a hybrid approach.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." The removal of, "storage locations" from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence.

We disagree with using, "provisioned access" as it is currently defined. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI, and for auditors to make that link to the repository of BCSI, to determine which has been provisioned for access.

Similar to "Provisioned access" noun, simply stating "BCSI" will make it intangible where keeping "storage locations" will make the requirement and its subparts tangible. See Q1 comment.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at third-party off-prem (*cloud based*) locations.

Use language similar to that in CIP-011 that addresses cloud storage for the proposed CIP-004.

Recommend creating a NERC Glossary defined term for "Provisioned Access."

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes

Document Name	
Comment	
Duke Energy agrees the proposed changes retain the flexibility for storage locations to be used as one way to meet the objective.	
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	
See comments in response to #9 below.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA and Indianca Comments.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	

MPC agrees that this approach provided entities with the flexibility to define their own internal procedures, which may include continuing to designate storage locations for BCSI to which individuals can have provisioned access. Provisioned access for those individuals can be authorized, verified, and revoked.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	Yes
Document Name	

Comment

OKGE supports comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E agrees with the modifications which make the Requirement more objective-based.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

We support EEI comments.

Likes 0	
Dislikes 0	

Response

David Hathaway - WEC Energy Group, Inc. - 6

Answer	Yes
Document Name	

Comment

Support comments made by EEI.

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

Southern agrees as with EEI and industry that this approach provided entities with the needed flexibility to develop and define their own internal procedures of what constitutes storage for current and future use.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon has elected to align with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	

Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
An organization should be able to define storage locations as well as decommission them, as long as appropriate controls are applied in both processes. The revised standard allows entities to apply controls at either the data level or storage level, without requiring either so long as data security is achieved.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Yes, this modification retains the flexibility for storage locations to be used as one way to meet the objective. However, absent clarifying language in the requirement regarding temporary and incidental access, the standard may inadvertently significantly expand the scope over the currently approved	

standard. This language is included in the Technical Rationale, but is not included in any enforceable language. It is recommended that additional clarification be added as outlined in the response to questions 1 and 2.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the approach provides entities with the needed flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term “storage locations” does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities’ access management programs. Such guidance would be helpful to ensure backward compatibility.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
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	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Black Hills does not find the distinction necessary. If consistent use of the language "obtain and use" then it should be evident that physical access to a computer, device, etc. does not constitute access to BCSI. The same logic that applies to a locked filing cabinet should apply to cyber access as well.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	No
Document Name	
Comment	
The IRC SRC observes that this approach appears to compensate for the removal of the concept of BCSI repositories. We suggest changing "physical access to physical BCSI" to "physical access to physical BCSI ***storage locations***" as "physical BCSI" limits the definition to the information itself (e.g. the drawings) and would not extend to include the protection of the storage location or repository as well (e.g. the drawer where the drawings are stored).	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	

GRE disagrees that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI.

Recommendation:
Adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy disagrees with the proposed changes, including a statement for both physical and electronic access only leads to further questions. CPS Energy propose defining what is considered Physical BCSI and Electronic BCSI as those terms are not defined by NERC – although should be understood Physical BSCI could be BSCI on printed medium, white board scribbles, photograph and electronic BCSI would be word docs, pdf, text file, digital photos – each person could define or scope the words physical and electronic in different ways.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	
Comment	
It is recommended that the SDT directly clarify the understanding that access to data or a tangible item that contains information does not equate to access to that information. The addition of such a clarification in the standard would simplify the understanding of the applicability of controls to the protection of BCSI.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
See our comments around “provisioned access” in Q5 AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
See our comments around “provisioned access” in Q5	
Likes 0	
Dislikes 0	
Response	

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
In the measures for R6.1, suggested evidence includes “the justification of business need for the provisioned access.” However, similar requirement 4.1 states “authorize based on need” but does not call out the justification of business need in the measures. 6.1 and 4.1 should be consistent in measures.	
Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree that the physical access only applies to physical BCSI since the controlling access to unencrypted BCSI has not been addressed. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI. We suggest adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnte for a Standard.	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
“Physical BCSI” is not a defined term. AEP recommends SDT to either define “physical BCSI” or add further clarifications in Requirement 6. AEP recommends using the existing language, “*Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*” under 6.1.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI. **Recommendation:**	

Adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
NO. Cloud services should be allowed. However, there is no need to make a distinction between electronic access and physical access.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Further clarification should be made to CIP-004-X Part 4.1.2 and Part 6.1.2 to address the difference between physical access to a Physical Security Perimeter that may house BCSI versus physical access to a physical piece of hardware that houses BCSI. Where does the physical piece of hardware that houses BCSI need to be stored?	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy agrees the proposed changes enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between “electronic access to electronic BCSI” versus “physical access to physical BCSI”.

Duke Energy does not agree with, and recommends removing, “and the justification of business need for the provisioned access” as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees where they would likely cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the distinctions made between “electronic access to electronic BCSI” and “physical access to physical BCSI”.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

“Physical BCSI” is not a defined term.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes

Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments, and has the following additional comments: For 6.2 and 6.3, OPG suggest to specify that the requirement is applicable to both physical and electronic provisioned access to BCSI similar to 6.1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	

Comment
Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	

Comment
Entergy does not oppose distinguishing electronic BCSI from physical BCSI; however, the change raises the question of how entities are to comply with 6.1.2. If someone prints out the ESP drawings on paper, must they then provide evidence of who has access to their office and how it was provisioned? Are we just going to expect that no hard copies of BCSI are created, or if so, they are only stored in a secure physical location with access controls? ***Specifying both electronic and/or physical access to BCSI will also mirror treatment of classified information – i.e. different protection strategies apply depending on the medium. It might be cleaner to just differentiate between electronic access and physical access. If you have physical access to a Cyber Asset, you still need to somehow get access to the electronic information stored on the physical asset - electronic info protection strategies apply. If the physical asset is paper (or maybe removable media) then you may rely more heavily on physical protection strategies.***

Likes 0	
Dislikes 0	

Response

Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx

Comment
In support of Tacoma Powers' comments. Attached.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
N/A.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
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	
Southern supports the distinction between “electronic access to electronic BCSI” and “physical access to physical BCSI.”	
Likes 0	
Dislikes 0	
Response	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the modifications and clarifications.	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
By this change, can it be clarified that an entity's IT service provider server rooms (where electronic BCSI is hosted) does not fall under physical BCSI.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	

MPC appreciates this distinction to enable the use of cloud service providers for entities that wish to use them and eliminate the interpretation that every possible encounter with BCSI cannot be access controlled in the way required by CIP-004, but would still be protected in another way under the entity's Information Protection Plan per CIP-011.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
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 NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

5. The SDT considered industry comments about defining the word “access”. “Access” is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define “access” in the NERC Glossary of Terms. Instead, the SDT used the adjective “provisioned” to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

CIP-004-X R2, R3, and R4 discusses authorized access. A user is to be authorized prior to being provisioned. If the CIP-004-X R6 requirements focus on provisioned users there is a gap of users who may be authorized and not yet provisioned. The SDT should chose to define authorized access in place of or in conjunction with provisioned access.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

NO. NERC Terms need a definition which is to be used for both CIP and O&P standards. Else Registered Entities will be subject to Regional Entity auditor interpretations not vetted by industry.

Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

1. Based on WAPA's disagreement of the term"provisioned access" and given that the SDT has defined "access to BCSI" in R6, the term "provisioned access" should be removed due to the creation of an unintended security loophole (See our comments in Q1).

2. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective "provisioned" adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

3. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." AEP suggests to use similar language from Part 4.1.3 as suggested in our response to Question #4 above. AEP recommends 6.1 use similar language to 4.1, i.e., "*Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*"

Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnte for a Standard.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Given that SDT has defined the “access to BCSI” in R6, the provisioned access needs to be removed since it has a unintended security loophole (See our comments in Q1).	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Providing the definition of “provisioned access” within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for “Provisioned Access.”	

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

If “provisioned” is needed, then what is non-provisioned access? SRP does don’t think “provisioned” is necessary, but adding it does not cause much concern. Access might need to be a defined term rather than using notes even if broken down between O&P and CIP.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards.

If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change.

Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific: “Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI”. Due to the first sentence of the question, it is not possible to define “access” alone, thus definitions for various types of access could be defined such as BCSI Access in this case.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	
Comment	

While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards.

If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change.

Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific: “Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI”. Due to the first sentence of the question, it is not possible to define “access” alone, thus definitions for various types of access could be defined such as BCSI Access in this case.

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	
Response	

Thomas Standifur - Austin Energy - 1,3,4,5,6

Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	

In support of Tacoma Powers' comments. Attached.

Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1,3,5

Answer	No
Document Name	
Comment	

CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 1,3,5,6

Answer	No
Document Name	

Comment

a. Given that the SDT has defined “access to BCSI” in R6, and the term “provisioned access” should be removed due to the creation of an unintended security loophole (See our comments in Q1).

b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective “provisioned” adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST notes that “provisioned” is not an adjective. Beyond that, “access” has already been given a contextual definition: “Obtain and use.” N&ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI and/or BCSI storage locations.

Likes 0	
Dislikes 0	

Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports not defining “access” as a NERC glossary term, as this could be difficult and have unintended consequences for other standards. MPC agrees that the use of “provisioned” and the note adds enough context to clarify what kind of access the requirements are about.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Provisioned access’ in Part 6.3 doesn’t necessarily trigger the removal of accesses granted maliciously or inadvertently, and accepts a security and reliability risk that is mitigated in today’s language. The use of provisioned access in Part 6.1 (authorize) and 6.2 (verify) is fine. Consider “… ability to access BCSI…” instead of “…ability to use provisioned access…” for Part 6.3 only	
Likes 0	
Dislikes 0	

Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the adjective “provisioned” and as noted in the comment for Question 1, will define what “provisioned” means to PG&E and following the definition in our implementation of the modifications.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	

David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with the use of term provisioned. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.	
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	
Southern agrees with the defining adjective of “provisioned” as the actions that may be taken to provide access to both electronic and physical BCSI. The “Note” further clarifies what possible specific actions may be considered as provisioned.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	

Answer	Yes
Document Name	
Comment	
ISO New England supports the clarification in the “Note”.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes

Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Suggest reiterating the “Obtain and use” qualifier in the Main R6 requirement. This well better explain what “Access” really means.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree that the Note clarifies provisioned access. We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes

Document Name	
Comment	
We agree that the Note clarifies provisioned access. We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Considering the R6.1 'Note,' the SDT should further clarify "provisioned access" in the IG/Technical Rationale and specifically address the "underlay" (CSP environment) from the "overlay" (SaaS, IaaS, PaaS) where "provisioned access" to BCSI is given.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	
From a technical standpoint, the addition of ‘provisioned’ provides clear delineation regarding the definition of ‘access’ in this context. Please reference the above comments in questions 1 and 2 regarding inclusion of clarifying language and guidance provided in the Technical Rationale within the standard. Additionally, it is recommended that the Note regarding provisioned access be moved to the main requirement in R6 where the term “provisioned access” is first used. This will also provide clarification that the note applies to all uses of the term within the requirement and not just part 6.1.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments, and has the following additional comments: Please provide additional clarification why the use of term “provisioned” is limited to access to BCSI and not also in Requirement 4 and 5.	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC has no concerns about adding “provisioned” to provide context, however, we are unsure if this helps clarify what constitutes access. Additional attempts to clarify “access” by the SDT may not be necessary. Individual entities have been successful in defining “access” for themselves and their programs whereby Attachment C and prior audit records can continue to support this approach.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Black Hills agrees with the decision, it should be evident that access is simply the ability to obtain and use, any further specifications beyond that should be an entity decision.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports not defining “Access” and agrees that providing a NERC glossary definition could have unintended consequences. EEI supports the decision to define “provisioned access” in the context of CIP-004 to be sufficient for the purposes of this standard but also recommends that this definition be elevated to the parent Requirement R6 given that “provision access” is used throughout this requirement. (See EEI comments to Question 1)	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 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	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 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	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

These proposed changes have not met the requirement of the SAR to prevent unauthorized access.

CIP-011 R1 Part 1.2, should be in alignment with CIP-004 R6 Part 6.1.

While detailed instructions are addressed in, “Measures” instead of in the “requirements.” Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in ‘Part 1.2 to broaden the focus on protecting and securely handling BCSI….’ in this current form it is contradictory with, ‘methods to protect’ in the Rationale, as their objectives are different.

Recommendation:

We suggest adding “prevent unauthorized access to BCSI” to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

“Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use.”

See the question to ‘broaden’ the focus of the language, and then the Technical Rationale says to be ‘explicit’…this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 & 1.4. This could result in a burden to industry here.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST agrees with the SDT’s decision to drop proposed Requirement R1 Parts 1.3 and 1.4. However, we disagree with the proposed changes to Parts 1.1 and 1.2, as we believe the existing language adequately defines the required elements of an Information Protection Program.

Likes 0	
Dislikes 0	

Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

While detailed instructions are addressed in, “Measures” instead of in the “requirements.” Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in ‘Part 1.2 to broaden the focus on protecting and securely handling BCSI….’ in this current form it is contradictory with, ‘methods to protect’ in the Rationale, as their objectives are different.

NVE suggests adding “prevent unauthorized access to BCSI” to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

“Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use.”

See the question to ‘broaden’ the focus of the language, and then the Technical Rationale says to be ‘explicit’…this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 & 1.4. This could result in a burden to industry here.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE is concerned that the proposed changes remove the concept of integrity, which is as equally important as the concept of confidentiality. The current approved language in Requirement Part 1.2 specifically supports the concept of integrity through the phrase “*storage, transit, and use.*” Texas RE asserts that such comprehensive language regarding BCSI storage, transit, and use – that is ensuring confidentiality and integrity – should continue to be included. Texas RE recommends adding “and integrity” after confidentiality in Requirement Part 1.2.

Additionally, Texas RE recommends the removal of “[i]mplementation of administrative methods” as an example of evidence for off-premise BCSI. If a Registered Entity intends to make use of third-party services for storing BCSI the Registered Entity is still responsible for ensuring the safety of the BCSI. A risk assessment or business agreement with the third-party vendor does not provide sufficient risk mitigation should the third-party vendor be compromised.

Lastly, as mentioned in response to Question #2, Texas RE recommends adding bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2. Texas RE recommends the following language:

1.2.1 - Method(s) to limit the ability of unauthorized individuals from obtaining or using BCSI. 1.2.2 - Method(s) to limit the ability of unauthorized individuals from modifying BCSI without being detected.

For those methods that use encryption, utilize an encryption key strength of at least 128 bits, in accordance with NIST.

For those methods that use hashing, utilize a hash function with an output size of at least 256 bits, in accordance with NIST.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

The proposed simplification is useful with the exception of the verbiage added to Requirement R1.2. Specifically, the term to mitigate the risk of compromising confidentiality is overly broad and ambiguous and could result in subjective interpretation during audits. The technical rational states that this change was made to “reduce confusion” but instead it has only added ambiguity. The existing language does not hinder the objectives of this SDT in any manner. Keeping this language consistent with the approved version of the standard will prevent unnecessary modification of existing CIP-011 programs, especially for those entities who have no desire to use cloud-hosted solutions.

As such, it is recommended that the language to R1.2 remain as follows:

Method(s) to protect and securely handle BCSI, including storage, transit, and use.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Thomas Standifur - Austin Energy - 1,3,4,5,6

Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx

Comment

In support of Tacoma Powers' comments. Attached.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	No
Document Name	

Comment

Integrity is an important security objective for 'Real-time Assessment and Real-time monitoring data' and is address in CIP-012. However, this should not negate the need to ensure the integrity of BCSI remains a security objective as well as confidentiality.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

We agree with comments from Duke Energy.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power supports the inclusion of method(s) as opposed to procedure(s); however, the inclusion of the objective of "mitigate the risk of compromising confidentiality" does not follow the current language provided in CIP-012 on order to maintain Standards consistency.

Therefore, Tacoma Power suggests the following alternative language:

“Method(s) to protect and securely handle BCSI to mitigate the risks posed by unauthorized disclosure and unauthorized modification of BCSI.”

The inclusion of unauthorized modification supports the fact that entities rely on the integrity of their BCSI in many instances, and should provide protections for data integrity where there is a risk associated with data integrity.

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We disagree with R1 Part 1.2 changes since these changes haven’t resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI. Using “mitigate the risks..” is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

We agree with the removal of language of “storage, security during transit, and use” from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	
Comment	

MidAmerican Energy agrees with removal of Parts 1.3 and 1.4. However, we are concerned with the lack of clarity of the language of Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI "becomes explicitly comprehensive." This question refers to a "broadened" focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added to Technical Rationale regarding expectations of the requirement, including the difference between version 2 and the proposed version X.

We agree with the removal of language of "storage, security during transit, and use" from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	
Comment	

Dominion Energy is concerned with the addition of "*to mitigate risks of compromising confidentiality*". This additional language seems to require that Registered Entities develop methodologies and processes to determine levels of risk. Furthermore, the term *mitigate risks* is very subjective and could be interpreted differently by the respective parties involved. This addition doesn't appear to address any risks or identified gaps. Please clarify the intent of the use of the language.

Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6

Answer	No
Document Name	
Comment	

AEP supports the removal of Requirement R1 Parts 1.3 and 1.4, and the minor adjustment made to Requirement R1, Part 1.1.

AEP has concerns that the adjustments made to Requirement R1, Part 1.2, made this requirement overly broad, especially considering the management of the off-premise BCSI. Specifically, AEP is concerned with the breadth and depth of L1 and L2 evidence that would be required to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise

BCSI. Further, it is not clear what would constitute acceptable methodologies or procedures (self-audit, independent audits, SOC1/SOC2 reviews, etc.) for AEP to validate a third party's control environment (provided the third party cooperates with AEP's request) sufficient to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise BCSI. Finally, it is not clear to what level AEP will need to document, monitor, and enforce controls implemented and administered by a third party who maintains AEP's BCSI off-premise.

AEP is also concerned with any unintended consequences from the proposed language, as it could be interpreted to mean any vendor's use of BSCI, even if it is stored on AEP's systems, and not BSCI that is stored, transmitted, or used by a 3rd party vendors on their system(s).

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

In CIP-011-X, Part 1.2, the proposed draft excludes risks related to data integrity. Omission of data integrity would require supplemental Practice Guides by the ERO Enterprise to determine what cloud environment risks are related to confidentiality vs. integrity. In practicality most data access risks overlap between those two legs of the CIA triad, and will be difficult or impossible to enforce some data risk scenarios with data confidentiality alone.
Also, the mapping document 'Description and Change Justification' indicates that the focus for CIP-011-X Part 1.2 was intended to be broader, but the change appears to be narrower than existing language. One or the other must be in error, but we are not sure which.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

We do not agree with R1 Part 1.2 changes since these changes haven't resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI.

Recommendations:

We suggest adding "prevent unauthorized access to BCSI" to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

"Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use."

Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	

NO. We agree with removing CIP-011XX R1 Parts 1.3 & 1.4.

We do not agree with adjusting Part 1.2.

Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

While more clear than the previously proposed CIP-011-3, the provided measures for CIP-011-X Part 1.2 it states, implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements). Business agreements and vendor service risk assessments does lead to confusion with CIP-013.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy generally agrees with the proposed changes of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality.

Duke Energy has concerns with the wording of measures for R1.2. ‘on-premise BCSI’ and ‘off-premise BCSI’ are open to interperetation. Is it the intent that a third party managed BCSI repository that is implemented on ‘on-premise’ servers not be subject to the ‘off-premise’ measures? Can a risk assessment determine the actual controls, physical, technical or administrative, needed?

Duke Energy recommends that for third party (or ‘off-premise’) managed or hosted storage, a risk assessment for physical, technical and administrative controls be performed and mitigating controls be implemented as determined.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees with removal of Parts 1.3 and 1.4. However, we suggest additional clarity of the language in Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI “becomes explicitly comprehensive.” This question refers to a “broadened” focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added to the Technical Rationale regarding the expectations of this requirement, including the difference between Draft 2 and the proposed Draft 3 version.

EEI agrees with protection of BCSI itself over the physical location in which BCSI is stored. We also support the removal of the language “storage, security during transit, and use” from this requirement. However, the language within the measure should also be removed. Furthermore, EEI does not support the use of the term “in use,” because this language is not necessary or auditable.

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
This draft is much more favorable than the previous. It's more open ended and the "confidentiality" statement aligns better with the spirit of what BCSI protection programs should aim to achieve.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the SDT's removal of parts 1.3 and 1.4 as retaining them in CIP-011 would have added another CIP standard to the scope of supply chain requirements. We view this as a good change.	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree with this simplification.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with this simplification.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	

Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes

Document Name	
Comment	
ISO New England agrees with this simplification.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
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	
Southern supports the deletion of CIP-011-X Requirement R1 Parts 1.3 and 1.4 and simplifying Parts 1.1 and 1.2. The SDT has made it clear the protection of BCSI itself is what is addressed here over where the BCSI is actually stored.	
Likes 0	
Dislikes 0	
Response	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E does not believe there is any double jeopardy between the proposed modifications to CIP-011-X and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC agrees with the proposed changes and believes that CIP-011 requires protection of BCSI no matter where it is located. To do this, entities must conduct assessments to understand what BCSI they have, where it can be found, how it transmits, what is done with it, and understand how confidentiality could be compromised at any of these times and locations in order to implement appropriate controls to protect it.

While MPC appreciates the reminder in the measures to consider BCSI that is located on-premises and off-premises, using these terms here may be confusing. MPC suggests including additional information in Technical Rationale or Implementation Guidance instead.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

In the Measures for R1.2, change "on-premise" to "on-premises” and “off-premise” to “off-premises”.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the extension of the 24-months implementation plan provided the CIP-004 R6.1 requirement to document justification of the need for authorization is eliminated.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC agrees with this approach.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the 24-month implementation plan and the ability for early adoption.	
Likes 0	
Dislikes 0	

Response

David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
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	
Southern agrees with the 24-month timeline. It will allow enough time to reach implementation.	
Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England agrees with aligning timelines.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	

Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with aligning timelines.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	

Comment	
We agree with aligning timelines.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Yes, 24 months is sufficient and aligning the changes with the Project 2016-02 SDT modifications will improve the efficiency and cost-effectiveness of the adjustments required to comply with these modifications.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

None.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Alliant Energy supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)

Answer	Yes
Document Name	

Comment

The IRC SRC acknowledges the SDT for incorporating our prior suggestion for added flexibility.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the proposal to extend the implementation plan to 24-months because changes will be necessary to align processes and training with the new requirements for both entities planning to utilize cloud services as well as those not planning to do so. EEI also supports the option for early adoption.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 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	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	

Comment	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
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	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	

Likes 0	
Dislikes 0	
Response	

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

Unknown fiscal impacts without a cost impact analysis and further clarifications.

PAC has strong concerns regarding the broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in significant impacts that are not cost-effective.

Standards should not be approved by until each SDT develop a detailed cost estimate.

There is no information to determine if the modifications are a cost-effective approach

Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST’s selection of “No” reflects our belief that currently proposed changes should be amended.

Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

Unknown at this time. The broadened approach to BCSI protections in CIP-011, could lead to potential high costs to an Entity.

Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP still holds to our comments from last time - the cost to implement will grow quickly with unclear requirements that lead to Responsible Entity concerns of proper interpretation. We would not say these are cost-effective at this time	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Unfortunately we wouldnt be able to properly answer this question at this time.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

At this time PG&E does not have information to determine if the modifications are a cost-effective approach.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment	
MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
The SDT has not provided a cost estimate. Consequently, we have no idea if the proposal is cost effective. Standards should not be approved by Industry until each Standard Drafting Team develops a detailed cost estimate (capital and maintenance). This means including internal controls, more staff, management/board approval, budgetting, revising all Internal Compliance Documents to account for the new standard or modifications, etc. All these changes end up costing real people, our customer, they certainly would not blindly tell the STD I just want that product and don't care what the cost is.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends removing “and the justification of business need for the provisioned access” as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees without need to cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The proposed changes appear to be backwards compatible, allowing entities to quickly adapt current compliance programs to incorporate the changes and are a substantial improvement over the last draft.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
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	
Southern agrees that the proposed changes are cost effective. There may be additional costs in the future for the use of different technology or applications but would be budgeted for any planned upgrades.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We think this is a cost effective way to address the issue.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	

Answer	Yes
Document Name	
Comment	
Any changes made result in a cost to industry.	
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	
See comments in response to #9 below.	
Likes 0	
Dislikes 0	
Response	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Hathaway - WEC Energy Group, Inc. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

N/A.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	

9. Please provide any additional comments for the SDT to consider, if desired.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
The proposed language is too ambigious and obligates entities to protect BCSI in any form, even though beyond its control. Should BCSI be shared with NERC/FERC, the proposed standard would require registered entities to extend their access management to include the copy of that information held by NERC/FERC. Subsequent requirements in CIP-011 would require reviews of access rights associated with that copy. The language should be re-scoped to focus on management of access to designated repositories, instead of the information itself.	
Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
The CIP-004-X and CIP-011-X proposal is more favorable than the previous CIP-004-7 and CIP-011-3 approach of moving access management of BCSI from CIP-004 and adding it to CIP-011.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	
Document Name	
Comment	
none.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	
The SDT should work to simplify but clarify the standards. Years down the road auditors make interpretations and companies need to be clear what is required. Secondly the SDT should look at ISO and NIST standards for guidance. Per our comments in question 1, WAPA recommends changing “provisioned access” to “access to BCSI” for whole R6 and its parts as suggested here: “Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:	

- For changes to R6 Part 6.2:

Verify at least once every 15 calendar months that all individuals with access to BCSI:

6.2.1. have an Is authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, as determined by the Responsible Entity.

- For changes to R6 Part 6.3:

For termination actions, remove the individual's ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action."

As we suggested in Q1, changing from "provisioned access to BCSI" to "access to BCSI" provides the clarity and flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	

Document Name	
Comment	
The SSRG wants to thank the drafting team for their time and efforts on this project.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	
No further comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

CIP-004-X R6 and CIP-011-X R1 have different applicability. In the Draft 3 language, BCSI pertaining to medium impact BCS without ERC must be protected (CIP-011-X R1), but access to this BCSI need not be controlled (CIP-004-X R6). Without mandated access controls, the entity will be left to determine what is an effective protection to BCSI pertaining to medium impact BCS without ERC. The SDT should consider revisiting the differences in applicability between CIP-004-X R6 and CIP-011-X R1. Since this issue is beyond the scope of the 2019-02 SAR, please add this concern to the list of SAR items for the next revision of CIP-004.

The Background sections of CIP-004-x and CIP-011-X should be moved to their respective Technical Rationale documents.

CIP-004-X Implementation Guidance: 1) Implementation Guidance for R2 states that “a single training program for all individuals needing to be trained is acceptable” which is in conflict with the language in R2, “appropriate to individual roles, functions, or responsibilities.” 2) Page numbers for R6 are incorrect. 3) Appendix 1 should be moved to the Technical Rationale document as it does not fit the requirements for Implementation Guidance.

Implementation Plan: The “Early Adoption” paragraph should make it clear that all of the updated Requirements must be adopted at the same time. An entity should not be permitted to early-adopt only parts of the revised Standards.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	
Document Name	

Comment

OKGE supports comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	
Document Name	

Comment

MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4.

While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E thanks the SDT for the effort in making the modifications objective based that will allow PG&E to implement them to fit our environment.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4.

While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	
Document Name	
Comment	

Resulting from our comments in Q1, we suggest changing “provisioned access” to “access to BCSI” for whole R6 and its parts.

Recommendations:

Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

For changes to R6 Part 6.2:

Verify at least once every 15 calendar months that all individuals with access to BCSI:

6.2.1. have an authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, as determined by the Responsible Entity.

For changes to R6 Part 6.3:

For termination actions, remove the individual’s ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

As we suggested in Q1, changing from “provisioned access to BCSI” to “access to BCSI” would provide the clarity and the flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes 0	
Dislikes 0	
Response	

David Hathaway - WEC Energy Group, Inc. - 6	
Answer	
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	
Document Name	
Comment	
Supportive of EEI comments on this project.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider's solution would likely be considered an EACMS based on the current definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case. Tacoma Power suggests modification of the EACMS NERC Glossary definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.	

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	
Document Name	

Comment

PNM Resources appreciates the work of the SDT and the opportunity to provide feedback.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

CIP-004 R6.2, in the Measures, suggest removing “Verification that provisioned access is appropriate based on need” – the need is confirmed by the authorization of access. Also, the measure should align with the requirement 6.2.2, which does not say “based on need”

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

Request clarification on Part 6.2’s Measures. Will auditing / enforcement expect every item? This Measure starts with “Examples of evidence may include.” Does the SDT mean this “may” is a “shall?” Recommend changing “Examples” to “Example.”

We look forward to seeing the final combined version of this update and the virtualization update.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	
Request clarification on Part 6.2's Measures. Will auditing/enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example." We look forward to seeing the final combined version of this update and the virtualization update.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to comment.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	

Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer

Answer	
Document Name	

Comment

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	
Document Name	

Comment

These changes are viewed as an overall improvement to the requirements around BCSI in CIP-004 and CIP-011. However, it would be more effective if these requirements were integrated into the existing framework of CIP-004 R4 and R5 rather than creating a new requirement R6. As it is now proposed, entities will need to recognize that authorizations are now covered in R4 and R6, periodic access reviews now exist in R4 and R6, and revocations are required in both R5 and R6. While the requirements are outlined reasonably, this separation creates a new burden on readability of the standards and training new staff regarding compliance expectations.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	

Document Name	
Comment	

Texas RE is concerned by now explicitly including the concept of confidentiality in CIP-011, Part 1.2, the SDT has inadvertently removed the concept of integrity from the scope of the proposed CIP-011. As noted in Texas RE's response to Question 6, the current approved language in CIP-011 that states "*storage, transit, and use*" in Part 1.2 supports the concept of integrity. Texas RE recommends adding "and integrity" after confidentiality in Requirement Part 1.2.

Texas RE also recommends including a bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2 should be established to ensure consistent application of the standard.

Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	
Comment	

CPS Energy does not have any additional comments at this time.

Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	
Comment	

ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee. In addition the ISO/RTO Council comments, ERCOT offers the following additional comments. First, with respect to Reliability Standard CIP-004-x, Requirement 6, Parts 6.1 and 6.2, the concept of roles should be allowed to be consistent with Requirement R4. This could be addressed in the requirement language or accompanying measure. If this is not permitted, ERCOT would appreciate an explanation explain why in the consideration of comments. Second, ERCOT believes the SDT should address the ability to use third-party audit reports in verifying the controls for third parties. Similarly, ERCOT would appreciate an explanation whether this is allowed or not, and why.

Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments, and has the following additional comments: CIP 004-X 4.1 requires entity to have a “process”; where 6.1 requires the entity to authorize but a “process” is not required. Both requirements seem to have similar intent with 4.1 applying to the Applicable System and 6.1 applying to BSCI. Please provide clarification whether the discrepancy is intentional.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	
Document Name	
Comment	
1. Resulting from our comments in Q1, we suggest changing “provisioned access” to “access to BCSI” for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3: • For changes to R6 Part 6.2: Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. have an Is authorization record; 6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity. • For changes to R6 Part 6.3: For termination actions, remove the individual’s ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action. We believe “access to BCSI” provides the flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible.	

2. The SDT may consider cleaning up the language to potentially the following language:

R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information - that collectively include each of the applicable requirement parts in CIP004-X Table R6 – Access Management for BES Cyber System Information.

[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

Revised Language Recommendations

6.1 Prior to authorization (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

6.1.1. Electronic access to electronic BCSI; and

6.1.2. Physical access to physical BCSI. Note: Access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights)

6.2 Verify at least once every 15 calendar months that all individuals with access to BCSI:

6.2.1. Have a current authorization record; and

6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

Alliant Energy supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)

Answer	
Document Name	2019-02_Unofficial_Comment_Form_BCSI Access Management_IRC SRC_05-10-21_FINAL.docx

Comment

CIP-011-X, Part 1.2, Measures: The IRC SRC recommends the SDT clarify that encrypted information, also known as cipher text, is not BCSI.

Examples of evidence for off-premise BCSI may include, but are not limited to, the following:

• Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, <delete cipher,> electronic key management); or

Note: MISO abstains from the response to item 9.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

N&ST has two additional comments, and associated recommendations, to respectfully offer.

The first comment is that in our opinion, the proposed changes do not address one of the project's stated goals, which is "…to clarify the protections expected when utilizing third-party solutions (e.g., cloud services)." N&ST is aware of the SDT's desire to avoid writing overly prescriptive requirements, such as was done in the first set of proposed revisions to CIP-011, but we nonetheless believe the issue of who is creating, and has the potential ability to use, authentication credentials such as encryption keys must be addressed in the Standards in one or more Requirements (vs. in "Measures" or guidance documents). We are aware of one Responsible Entity that was found by a Regional Entity audit team to be out of compliance with CIP-004 for storing BCSI in the cloud and relying on the cloud service provider's default encryption. Simply dropping "storage locations" from CIP-004 would not, by itself, have helped the Responsible Entity avoid this problem. N&ST therefore recommends the following or similar language be added to either CIP-004 or CIP-011:

“The Responsible Entity shall ensure that all individuals, including those affiliated with third parties such as vendors and cloud service providers, who possess the means to obtain and use BCSI that is protected by one or more electronic and/or physical access controls (login credentials, unlock passwords, encryption keys, cardkeys, brass keys, etc.) have been authorized in accordance with CIP-004 requirements.”

N&ST’s second comment is that we are concerned there is insufficient clarity with regards to what distinguishes “provisioning” from “sharing.” During the recent SDT webinar, a member of the SDT gave listeners a good example: (paraphrasing) Person A, who has been provisioned access to a file cabinet and has a key, opens it and gives a BCSI document to Person B, who has not been authorized for access to the file cabinet and cannot open it. Person A has shared BCSI with Person B. The SDT has already created a contextual definition of “access to BCSI.” N&ST recommends that a similar contextual definition of “sharing” be added to either CIP-004 or CIP-011, working off the example the SDT itself created.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

Recommend creating a NERC Glossary defined term for “Provisioned Access.”

“Physical BCSI” is not a defined term.

“Storage Locations” is no longer explicitly stated.

The language should be re-scoped to focus on management of access to designated repositories

We appreciate all the time and effort given to this project to develop these revisions/changes.

However, if you are approving a new set of Standards, we recommend that the Technical Guidance is also published at the same time. The excessive delay between these publications, is causing industry confusion.

The VSL – this is excessively severe (Proposed VSLs are based on a single violation and not cumulative violations.)

Recommend:

Use the same language as previously in R4:

R4: Operations Planning and Same Day Operations – VRF Medium The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)

Authorize happens *prior* to provisioning access R6.R1 – See Note: The SDT is relying HEAVILY on the CMEP guide for definition parameters, and not the STD language.

Clarify BOTH CIP-004 & CIP-011 requirements relating to managing access and protecting BCSI.

Likes 0	

Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI is concerned with having two separate requirements within CIP-004-X that address access removal. (See Requirement R5 (BCS) and R6 (BCSI) While we understand the intent and reasons for this change, often access is provided to individuals for both BCS and BCSI and any failure in the termination of access in these cases will result in two violations for the same error. We recommend that this issue be reconciled.	
Likes 0	
Dislikes 0	
Response	
Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
See comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
Likes 0	
Dislikes 0	
Response	

Comments received from Basin Electric Power Cooperative

1. *The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

   ☐ Yes
   ☒ No

   Comments: The term "provisioned access" adds another undefined term to the NERC standards and doesn't provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.

   a. "Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas "access to BCSI" occurs when an individual has both "the ability to obtain and use BCSI," we recommend changing "provisioned access" to "access to BCSI".
   b. The term "unless already authorized according to Part 4.1" should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.
   c. The use of "provisioned, provision or provisioning" of "access," regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the "provisioned" configurations of entity BES Cyber System Information repositories in order to "verify" the "authorization" of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle
   d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3rd party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)

   Recommendations:

   1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
   2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 " to prevent unauthorized access to BES Cyber System Information." This allows entities to determine the risk and methods to protect BCSI
4. Consider using "authentication systems or encryption of BCSI" for personnel accessing electronic BCSI on cloud prem providers locations.

2. *The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

a. We agree to adding "obtain and use" language to clarify what constitutes an access to BCSI, but disagree to the use of "provisioned access". After clarifying the access to BCSI, the language "provisioned" should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

Recommendations:

1. Only use the term "access" as recommended in Q1

3. *The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal*.

☐ Yes
☒ No

Comments:

a. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1).

b. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

4. *To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets "obtain and use" condition and constitutes an access to BCSI.

Recommendation:

Adding "Physical access to unencrypted electronic BCSI" to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

5. *The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

a. Given that the SDT has defined "access to BCSI" in R6, and the term "provisioned access" should be removed due to the creation of an unintended security loophole (See our comments in Q1).
b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective "provisioned" adds

further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

6. *In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.*

☒ Yes
☐ No

Comments: does not explain Prior language in the Rationale for Modifications to Requirement R1, Part 1.2 "By removing this language, methods to protect BCSI becomes explicitly comprehensive."

7. *The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

☒ Yes
☐ No

Comments:

8. *In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?*

☒ Yes
☐ No

Comments:

9. *Please provide any additional comments for the SDT to consider, if desired.*

Comments:

1. Resulting from our comments in Q1, we suggest changing "provisioned access" to "access to BCSI" for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:
   - For changes to R6 Part 6.2:

     Verify at least once every 15 calendar months that all individuals with access to BCSI:
     6.2.1. have an Is authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity.

- For changes to R6 Part 6.3:

  For termination actions, remove the individual's ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

  We believe "access to BCSI" provides the flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible.

2. **The SDT may consider cleaning up the language to potentially the following language:**
   R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information - that collectively include each of the applicable requirement parts in CIP004-X Table R6 – Access Management for BES Cyber System Information.

   [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

Part	Revised Language Recommendations
6.1	Prior to authorization (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Electronic access to electronic BCSI; and 6.1.2. Physical access to physical BCSI. Note: Access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights)
6.2	Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. Have a current authorization record; and 6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2019-02 BES Cyber System Information Access Management (Draft 3)
Comment Period Start Date:	3/25/2021
Comment Period End Date:	5/10/2021
Associated Ballots:	2019-02 BES Cyber System Information Access Management CIP-004-7 AB 3 ST 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 3 ST 2019-02 BES Cyber System Information Access Management Implementation Plan AB 3 OT

There were 64 sets of responses, including comments from approximately 157 different people from approximately 98 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, 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, contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Questions

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?

9. Please 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
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities	4	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						(Tacoma, WA)		
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power Incorporated	1,3	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO,WECC	Southwest Power Pool Standards Review Group (SSRG)	Kim Van Brimer	SPP	2	MRO
					Jim Williams	SPP	2	MRO
					Matt Harward	SPP	2	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shannon Mickens	SPP	2	MRO
					Alan Wahlstrom	SPP	2	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy- FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
of Chelan County						of Chelan County		
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company -	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company -	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Southern Company Services, Inc.						Southern Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6, 7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
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	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
						Virginia Power		
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The use of provisioned access is not addressed in CIP-004-X Requirement 5. The CIP-004-X requirements should use consistent terminology.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. CIP-004-X (and also CIP-004-6, the currently enforceable standard) R4 and R5 is/was already properly scoped to the kind of access to be authorized, verified, and revoked (i.e., electronic access to applicable cyber systems and unescorted physical access into a Physical Security Perimeter). Although this is also provisioned access, it is not necessary to add the qualifier to R4 and R5. However, it is necessary to include the word "provisioned" to scope the kind of access to BCSI the R6 requirements pertain to.	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No

Document Name	2019-02_Unofficial_Comment_Form_03252021_Information-Protection-NSRF-draft-1_JC.docx

Comment

Comments: WAPA believes the SDT is moving in the correct direction from the past version. WAPA does not support the term "provisioned access" as it is a non-definable term which has the potential to confuse regulators (auditors, risk, enforcement, FERC, NERC, etc…) and industry. The term also does not address the requirements in the SAR for entities storing BCSI off-prem (such as cloud data centers).

"Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas "access to BCSI" occurs when an individual has both "the ability to obtain and use BCSI," we recommend changing "provisioned access" to "access" that ensures only authorized individual can possess BCSI.

The use of "provisioned, provision or provisioning" of "access," regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the "provisioned" configurations of entity BES Cyber System Information repositories in order to "verify" the "authorization" of such provisioned access.

The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers may not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI without litigation, yet entities will be asked to provide this information for an entire audit cycle

Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI; 6.1.2 Physical access to physical BCSI; 6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4). 3. Consider using the perspective of language in CIP-011 " to prevent unauthorized access to BES Cyber System Information." This allows entities to determine the risk and methods to protect BCSI 4. WAPA recommends addressing the two potential controls for access to off-prem BCS, 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. This could be as simple as: Implement at least one control to authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes: 6.1.1. Electronic access to electronic BCSI; 6.1.2 Physical access to physical BCSI; 6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. **Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI,**	

especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program. **The CIP-004 standard includes contractors and service vendors, so cloud service provider personnel must be included in an entity's access management program (authorize, verify, and revoke provisioned access).**	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Marty Hostler.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

In AEP's opinion, the updated language leaves room for interpretation. It might be simplistic to refer to the subparts of R6 instead of using specific words from the subparts.

The updated Requirement 6 would read: "Each Responsible Entity shall implement one or more documented access management program(s) to *meet subparts of R6 for provisioned access* to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]."*

Likes 0	
Dislikes 0	

Response: Thank you for your comment. It is understood that all subparts follow suit of the parent requirement. The parent requirement is requiring that an entity authorize, verify, and revoke access for the respective parts. In addition, the SDT added authorize, verify and revoke during the last round of edits based on entities requesting additional clarification for provisioned access.

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment

We disagree with "provisioned access" since there is a security concern where it only requires authorization for a provisioned access. If an access to BCSI is not provisioned, it means no authorization is required. This doesn't meet the goal of SAR for controlling access to BCSI. Given that R6 has defined "access to BCSI" as an individual has both the ability to obtain and use BCSI, we suggest changing "provisioned access" to "access" that ensures only authorized individual can possess the BCSI. Also "unless already authorized according to Part 4.1" should be removed as having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.

Recommendations: We have the following suggested language for R6 Part 6.1: Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes: 6.1.1. Electronic access to electronic BCSI; 6.1.2 Physical access to physical BCSI; 6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

Likes 0	
Dislikes 0	

Response Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. **Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.**

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Providing the definition of “provisioned access” within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for “Provisioned Access.”	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
•"Prior to provisioning, authorize **provisioned** access"? Wouldn't it be more appropriate to remove "provisioned" in 6.1.1 and 6.1.2? How can an entity authorize provisioned access if it hasn't been provisioned yet?	

• R6 requires provisioned access to BCSI to be authorized based on need, reviewed, and revoked upon a termination action. • R6 makes no mention of “Transfers or reassignments”. R5 does not address revoking provisioned access to BCSI either, therefore entities are not required to revoke provisioned access to BCSI unless they are terminated. • Provisioned access to BCSI does not require an individual to have Cyber Security Awareness training or a PRA. Could an individual have no access to a BCS but have all of the information relating to the BCS. •In the Note section of R6.1 “Provisioned access is to be considered the result of the specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys).” {C}- Recommend changing the e.g., section to read “physical keys or access control key cards, user accounts and associated rights and privileges, encryption keys).	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Response by topic is as follows: **1) The term “provisioned access” is to be read as a noun/concept. The Note that had been included in the requirement defines what provisioned access means in the context of this requirement. Responsible Entities are to authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized. In addition, the “note” has been removed from the subpart and the language that was within the note has been moved up into the parent requirement R6.** **2) Current CIP requirements related to BCSI are not concerned with “Transfers or reassignments” and neither are the requirements that this SDT has drafted. Modifying the BCSI requirements to address this concern is beyond the scope of this SAR. However, we do not believe it is accurate to say that provisioned access to BCSI is not required to be revoked unless someone is terminated, either in the current or drafted requirements. Responsible Entities are required to review BCSI access once every 15 months and take appropriate actions, including removal of access.** **3) Regarding Cyber Security Awareness Training, this is not required for access to BCSI in the current CIP requirements; adding that requirement is beyond the scope of this SAR.**	

4) Regarding the modification of the note to say "access control key cards", the SDT considered but did not make this revison to our final updates. Adding additional adjectives may cause confusion or limitations to the SDT's intent and the broader language.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While the SDT did well in clarifying the intent of the provisioning, we do not feel a "Note" inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. In addition, the "note" has been removed from the subpart and the language that was within the note has been moved up into the parent requirement R6.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

While the SDT did well in clarifying the intent of the provisioning, we do not feel a “Note” inserted into the requirement is sufficient to serve as a NERC definition. See Q5 comments. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. In addition, the “note” has been removed from the subpart and the language that was within the note has been moved up into the parent requirement R6. Please see the SDT’s response to ACES.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to Tacoma Power.	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	2019-02_Unofficial_Comment_Form_Final Draft.docx
Comment	

For the purposes of providing for cloud storage and processing of BCSI information, the proposed changes are sufficient to provide for its use. However, the changes are silent with regard to the authorized incidental access of BCSI in a physical environment such as a meeting. It is recommended that clarification be provided in the requirement language for such circumstances. This is addressed in the Technical Rationale: however, it was not included in the standard.

The following modification is suggested to the Note in requirement part 6.1:

Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6. Based on the comments received and ballot results, the SDT determined the language is sufficient as written.

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	

Part 6.1 perhaps should read as follows:

Unless already authorized according to Part 4.1, authorize provisioned access based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

CPS Energy suggests creating a NERC Glossary defined term for "Provisioned Access" instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, "obtain and use" should be included in the definition.

Likes 0	
Dislikes 0	

Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. In addition, the "note" has been removed from the subpart and the language that was within the note has been moved up into the parent requirement R6.

Michael Brytowski - Great River Energy - 1,3,5,6

Answer	No
Document Name	

Comment

The term "provisioned access" adds another undefined term to the NERC standards and doesn't provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.

a. "Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI.

Given the R6 definition whereas “access to BCSI” occurs when an individual has both “the ability to obtain and use BCSI,” we recommend changing “provisioned access” to “access to BCSI”.

b. The term “unless already authorized according to Part 4.1” should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.

c. The use of “provisioned, provision or provisioning” of “access,” regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the “provisioned” configurations of entity BES Cyber System Information repositories in order to “verify” the “authorization” of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle

d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3rd party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)

Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.

2. Consider the following language for R6 Part 6.1:

Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

6.1.1. Electronic access to electronic BCSI;

6.1.2 Physical access to physical BCSI;

6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).

3. Consider using the perspective of language in CIP-011 " to prevent unauthorized access to BES Cyber System Information." This allows entities to determine the risk and methods to protect BCSI 4. Consider using "authentication systems or encryption of BCSI" for personnel accessing electronic BCSI on cloud prem providers locations	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST notes that words can only be nouns, verbs, adjectives, etc. on an individual basis. Calling any two-word phrase a noun is grammatically incorrect. Beyond that, the phrase, “provisioned access,” as used in proposed CIP-004 requirements, is itself grammatically incorrect by virtue of the fact “provisioned” is the past tense of the verb, “provision.” It is not an adjective. An individual can be given access or can be provisioned access but cannot be given provisioned access. Since the SDT has adopted NERC’s informal definition of “access to BCSI” as the ability to “obtain and use” it, N&ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI (or BCSI storage locations), dropping the misunderstood and grammatically incorrect “provisioned access.”	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed change to “provisioned access” and that the entity will determine how that provisioning will occur.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA and Indiana Comments	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Please see the SDT’s response to WAPA.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	

Comment	
MPC agrees that this change provides greater clarity regarding the intent of this requirement and understands that it is the provisioned access that must be authorized, verified, and revoked.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	EEI Near Final Draft Comments_ Project 2019-02_Rev_0f_For Review FOR MEMBER REVIEW.docx
Comment	
OG&E agrees with EEI's comments	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	

OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Assuming that "provisioned access" means when someone gains and keeps BCSI access? Meaning if someone sees (screen sharing in view mode only) does not fall under "provisioned access"?	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Items such as see/hear/memorize type encounters with BCSI such as a red only screen share do not constitue access under CIP-004. Instead, this falls under the realm of information sharing that is subject to the Information Protection Program within CIP-011 and is accomplished through an entity's handling methods.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language to the parent requirement R6.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the proposed modifications. PG&E will define what is “provisioning of access” for our environment and will not need a defined NERC term since a NERC term may not cover all possible conditions for PG&E.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

Move the note to the parent requirement (R6), since it applies to more than 6.1, and remove the word “Note.”	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language from the note to the parent requirement R6.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to EEI.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	

Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree with the proposed change. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.	
Likes 0	
Dislikes 0	
Response: Thank you for your support. Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees as with EEI that the change provides greater clarity regarding the intent of the Requirement.	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Kinte Whitehead - Exelon - 3	

Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Be careful adding "NOTES" to requirements. If the purpose is to increase clarity, then consider re-writing the requirement to improve clarify. NOTES may become overused across CIP standards and cause confusion.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language from the note to the parent requirement R6.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	

IESO supports the comments submitted by NPCC.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We support these changes.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that "provisioned access" is an improvement and supports the proposed change.	
Likes 0	

Dislikes 0	
Response: Thank you for your support.	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy agrees that this change provides greater clarity regarding the intent of this Requirement.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC Regional Standards Committee.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The ISO/RTO Council Standards Review Committee (IRC SRC) acknowledges the SDT for addressing our prior concerns surrounding the lack of clarity associated with "provision of access."	
Likes 0	
Dislikes 0	
Response: Thank you for the acknowledgment, the SDT appreciates your support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PAC requests the SDT provide better definition of "provisioned access" than what was currently provided in Part 6.1	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Based on the comments received and the ballot results, the SDT considered comments and determined the language is sufficient.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that this change provides greater clarity regarding the intent of this Requirement. However, use of the term "note" creates ambiguity because it is not clear whether the language in the note creates mandatory obligations. The use of the word "note" should be	

removed and the language contained in the note in Requirement R6, Part 6.1 should be elevated to the parent Requirement R6 because the term “provisioned access” is used in other parts of Requirement R6. Additionally, the note language should be strengthened for additional clarity (e.g., “is to be considered” may not be clear for industry to understand what the note means)	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language from the note to the parent requirement R6. Based on the comments received and the ballot results, the SDT considered comments and determined the language is sufficient.	
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	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Northern California Power Agency - 3,4,5,6 - WECC	

Answer	
Document Name	
Comment	
disregard	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE seeks clarification regarding the scope of the revised CIP-004, Part 6.1. Specifically, Texas RE interprets "provisioned access" to include all instances in which an individual is "provisioned access" to BCSI. Accordingly, accidental or mistaken provisioned access would be within the scope of the requirement. Conversely, compromise of BCSI without any specific entity actions to provide the means to access BCSI (such as a data breach) would not be within the scope of the proposed requirement. Texas RE inquires as to whether this is the SDT's intent.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. With regards to the human performance examples of accidental or mistaken provisioned access, it would be the understanding that an entity would correct and self-report in those instances. CIP-004 requirements are designed to manage that which the entity controls (authorization, verification, provisioning, and revocation), and not designed to	

address mallicious acts such as data exfiltration/breaches; the SDT intention is for CIP-011 protections to serve to detect, prevent, deter those conditions.	
Doug Peterchuck - Omaha Public Power District - 1	
Answer	
Document Name	2019-02_Unofficial_Comment_Form_Information-Protection-OPPD.docx
Comment	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Please provide additional clarification in the Standard, and in the technical rationale. Does the term, 'use' allow a user to unencrypt? Potential here for resulting in a potential data manipulation. Recommendation: Only use the term, "access." See the new R6 versus the former R4 language changes for clarification.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. If the person can unencrypt the data, they would have provisioned access. The SDT determined that the term "provisioned" would be the appropriate phrase instead of access. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	
GRE agrees to adding “obtain and use” language to clarify what constitutes an access to BCSI, but disagree to the use of “provisioned access”. After clarifying the access to BCSI, the language “provisioned” should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1). Recommendations: 1. Only use the term “access” as recommended in Q1	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDT determined that the term “provisioned” would be the appropriate phrase instead of access. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy suggests “obtain and use” be included within R6 statement.	

"Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access **that grants the ability to obtain and use** BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The phrase "obtain and use" is included in Requirement R6. Based on the recent comments and ballot results, the SDT determined that the language currently drafted accomplishes the objective.	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
Additional clarity is needed for what constitutes access by "obtain and use". Specifically, clarify what "use" means by defining the point at which information is considered "used". Does "use" mean immediately when the information is read by someone, or does it mean when the information is applied for some purpose? For example, if someone obtains information and can read it, and there are additional physical or electronic controls in place to prevent unauthorized use of the obtained information, do those controls then prevent "access to BCSI" based on the premise that information must be obtained and used to constitute access to BCSI?	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	

Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Tacoma Power.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	

Integrity should also be included as a security objective for BCSI in addition to confidentiality. Removing "obtain and use" is not consistent with the ERO Enterprise CMEP Practice Guide nor is it consistent with

https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

In the R6 Requirement language "To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI."

- This statement contradicts the Requirement of R6.1. If a user must concurrently have the ability to both, obtain and use BCSI how does that provide the entity the ability to authorize based on need, as determined by the Responsible Entity?

- The webinar on 4/27/2021 attempted to clarify what the right and left lateral limits of BCSI "use" could be, but further clarifications might be needed to ensure a consistent approach is expected for authorization and provisioning.	
Likes 0	
Dislikes 0	

Response: Thank you for your comment.

1) **Regarding the comment speaking to adding Integrity as a security objective for BCSI. That is beyond the scope of this SAR and it is not the intent of the SDT to include Integrity requirements/objectives in this draft. The security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also reduced and the security goal has been achieved.**
2) **Regarding the comments speaking to the "obtain and use" language, the comment is somewhat confusing. The SDT did not remove the obtain and use language. In the context of this requirement, an individual is considered to have provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. Putting the requirement language and the clarification of what access means together, a Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.**
3) **Regarding the comment speaking to the limits of BCSI "use", the SDT will consider this feedback when drafting implementation guidance. The SDT also invites you, and other entities, to also draft implementation guidance that would speak to your concern.**

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Access needs to be better defined, in particular the phrase “use BCSI” – being able to view a document or taking advantage of the information in the document. Is it “I have access to the file but not able to open it”, or is it “I have BES cyber system IP address, but no ability to get to those systems because there are other controls preventing me from using that information”?

Where is it in the standard that this is spelled out as a clear definition – “two-prong test”? This is not clear in the question above – shouldn’t the requirement be more clear?

Likes 0	
Dislikes 0	

Response: Thank you for your comment. In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. The SDT also invites you, and other entities, to also draft implementation guidance that would speak to your concern.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

The placement of the “obtain and use” statement gets lost within the construct of the Requirement Language, it appears as an add-on to the high level R6 language.

Suggested alternative:
“Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke the provisioned access that grants the ability to obtain and use BCSI pertaining to the “Applicable Systems” identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-X Table

R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]"	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response: Thank you for your comment. Based on the favorable vote from industry, the SDT determined the language of R6 aligns with the CMEP Practice Guide and accomplishes the objective.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We agree to adding "obtain and use" language to clarify what constitutes an access to BCSI, but disagree to "provisioned access". After clarifying the access to BCSI, the language "provisioned" should be removed since it has a security flaw (See our comments in Q1).	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is,	

grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy is of the opinion that the terms“obtain and use” are ambiguous. We suggest additional language that provides for the Registered Entity to have the felxibility to define how these terms are applied by adding some additional language to the proposed Requirement as follows: …*an individual has both the ability to obtain and use BCSI as defined by the Registered Entity.*	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. The SDT also invites you, and other entities, to also draft implementation guidance that would speak to your concern.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Marty Hostler.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

1. We agree to adding "obtain and use" language to clarify what constitutes an access to BCSI, but disagree to the use of "provisioned access". After clarifying the access to BCSI, the language "provisioned" should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

Recommendations:

1. Only use the term "access" as recommended in Q1

Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and	

approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
A user can have provisioned access to obtain BCSI and not use it. The Registered Entity is currently receiving an authorization for a user based on need to access BCSI. Access to BCSI is enough to constitute an authorization regardless of use. While this clarification assists in the context of third-party solutions it does not provide clarity for electronic or physical access to BCSI.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the clarifying language contained in the two-prong test (i.e., “obtain and use”) provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. EEI also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills would recommend that 6.1’s “Note” section use the same language as R6 opening paragraph. Specifically “ability to obtain and use” should be used whenever possible, in this instance the “Note” section may read like this, “Provisioned access is to be considered the result of the specific actions resulting in an individual’s ability to obtain and use BCSI.”	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language from the note to the parent requirement R6.	

In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment
ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)

Answer	Yes
Document Name	

Comment
The IRC SRC supports the reinstatement of "obtain and use" concepts.

Likes 0	
Dislikes 0	

Response: Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC SRC.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	

Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NVE agrees that the clarifying language contained in the two-prong test (i.e., “obtain and use”) provides reasonable protections for controlling access to BCSI, particularly as it relates to BCSI that might be stored in a third-party cloud environment. NVE also agrees that having physical access to BCSI but not having the ability to use it is impractical because it does not represent access from a functional standpoint or for a useful purpose.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Texas RE agrees that the two-pronged test is an improvement over the existing language. Texas RE is concerned, however, that the verbiage "obtain and use" is subject to further interpretation. One approach could be to clarify the verbiage to read: "*the authorized ability to retrieve, modify, copy, or move BCSI*". Alternatively, Texas RE recommends creating bright line criteria establishing what it means for the BCSI to be usable.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. The SDT also invites you, and other entities, to also draft implementation guidance that would speak to your concern.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
The 'obtain and use' language introduced provides valuable clarification with regard to provisioning and deprovisioning of access and provides context that will enable clearly defined opportunities to leverage cloud services. However, as drafted, the standard effectively provides different explanations for "access" versus "provisioned access." It would increase clarity if these explanations were combined. It is recommended that the note explaining provisioned access be moved to the main requirement so that all explanatory statements regarding access or provisioned access are in the same place. In this manner, it is clear that the clarifications to "provisioned access" apply across all parts of requirement R6.	

Consistent with our recommendation to question 1 regarding incidental access, this would modify the main requirement of R6 as follows:

…To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). Provisioned access does not include temporary or incidental access when a specific mechanism for provisioning access is not available or feasible such as when an individual is given, merely views, or might see BCSI such as during a meeting or visiting a PSP, or when the BCSI is temporarily or incidentally located or stored on work stations, laptops, flash drives, portable equipment, offices, vehicles etc.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response: Thank you for your comment. The SDT determined that the language is clear as written based on the favorable votes received from industry and that an inclusion is not needed at this time. The SDT did remove the note from 6.1 and added the language to the parent requirement. Plese see those edits.

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer

Answer	Yes
Document Name	

Comment

Evergy supports and endorses the comments filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Entergy supports the inclusion of the "obtain and use" language from the CMEP Practice Guide. This language clarifies that users with "access" for purposes of the requirement must be able to obtain and use BCSI, which addresses industry's concern regarding encrypted data. In particular, the prior language could present a grey area where a user could receive an encrypted BCSI item and be considered as having the BCSI even though they (conceivably) could not use it. This approach aligns with Entergy's interpretation under both its current BCSI program, as well as the guidance and position we are pursuing for BCSI in the cloud	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to ACES.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We support the update to this Requirement language.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Support the update to this Requirement language.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Becky Webb - Exelon - 6	
Answer	Yes

Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this update.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	

Dislikes 0	
Response: Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that for access to occur, a user must both obtain BCSI and possess the ability to use BCSI according to the CMEP dated April 26, 2019.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees that the clarification is sufficient.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	

Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP agrees with the addition of "obtain and use" language in R6 parent requirement, as this is in alignment with AEP's BCSInfo program.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	

Comment	
The SPP Standards Review Group (SSRG) recommends the word “use” have clarity supplied around the term.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. The SDT also invites you, and other entities, to also draft implementation guidance that would speak to your concern.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC appreciates the SDT’s efforts to include the concept from the CMEP Practice Guide. However, we would prefer the language be more specific to CIP-004, rather than re-introduce the broader “access” concept that goes beyond CIP-004 by using this language instead: “An individual is considered to have provisioned access to BCSI if they concurrently have the means to both obtain and use the BCSI (e.g., an individual who obtains encrypted BCSI but does not have the encryption keys does not have provisioned access).” The example is helpful in understanding what is meant by “obtain and use.”	
Likes 0	
Dislikes 0	
Response: Thank you for your support and comment. Based on the favorable votes, the team determined that the current language is well understood among industry and made some non-substinative changes. Please see the minor changes made by the SDT to CIP-004.	

Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA Contents.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Please see the SDT's response to WAPA.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees the proposed changes make it clear that both parameters of the two-pronged test for "obtain and use" must be met to constitute "access" to BCSI.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Storage locations identified for using BCSI is reference in CIP-011-X. CIP-004-X and CIP-011-X should provide consistent terminology.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Utilizing a designated storage location is still an acceptable method to both control access to BCSI (CIP-004-X) and to protect and securely handle BCSI (CIP-011-X). Even though the use of the term storage location is only referenced in the CIP-011-X Measures, the SDT did not intend that use of such was limited to CIP-011-X. Both the Webinar materials and CIP-004-X Technical Rational both stress that storage locations are still an acceptable method to control access to BCSI.	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

1.

i. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using “provisioned access” (See our comments regarding “provisioned access” in Q1).

ii. The requirement to provide lists of personnel with “provisioned access” would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	

Response: The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to Marty Hostler.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." Removing "storage locations" from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence. Similar to "Provisioned access" noun, simply stating "BCSI" will make it intangible where keeping "storage locations" will make the requirement and its subparts tangible.

AEP understands the intent but it is not clear based on how it is currently worded. AEP requests SDT to provide further clarification on the intent and to provide better definition on "provisioned access" than what was currently provided in Part 6.1 ("Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).)" AEP also recommends SDT to focus on auditable methods to protect BCSI at 3rd party off-premise (cloud) locations.

AEP currently defines what constitutes as storage locations in CIP-011-2 R1 information protection program, but for other smaller entities this may become further complicated to define besides managing access to BCSI storage locations.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
To ensure a consistent understanding of the issues surrounding information storage on the cloud, Dominion Energy suggests using language similiar to that in CIP-011 that addresses cloud storage in the proposed CIP-004.	
Likes 0	
Dislikes 0	
Response: The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1). The objective of SAR and NERC CMEP BCSI guidance is to	

prevent unauthorized access to BCSI rather than “provisioned access to BCSI”. Using “provisioned access to BCSI is lowing the bar for the BCSI authorization doesn’t meet the goal of SAR for controlling unauthorized access to BCSI. Also “provisioned access” is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. The focus of the BCSI requirements in CIP-004 is managing individuals’ access to BCSI where access can be provisioned, and the focus of CIP-011 is protecting BCSI from unauthorized access no matter where it is located.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider’s solution would likely be considered an EACMS based on the current EACMS definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case. Additionally many modern cybersecurity tools such as local endpoint protection	

systems, now make use of Cloud services to provide additional context to the information seen on local systems, and require that much of the system log data be pushed to the Cloud to enable this analysis. Tacoma Power suggests modification of the EACMS definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response: Thank you for your comment. The EACMS modification is outside the scope of this project's SAR.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using "provisioned access" based on our concerns in Q5.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No

Document Name	
Comment	
While we agree with the SDT retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, we disagree with using “provisioned access” based on our concerns in Q5. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Spliting EACMS is outside the scope of this project’s SAR.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	

Answer	No
Document Name	
Comment	
NVE agrees that the approach provides entities with the additional flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term "storage locations" does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities' access management programs. Such guidance would be helpful to ensure backward compatibility.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	

CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to the ISO/RTO Council SRC.	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	

a. GRE agrees to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1).

b. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)

Answer	No
Document Name	

Comment

The IRC SRC is concerned that keeping "storage locations" without defining it in the standard or the NERC Glossary will require entities to define it for themselves. This will create a variety of interpretations throughout the regions.

The IRC SRC recommends the SDT consider defining the term "storage locations" to indicate that storage locations may be physical locations or virtual locations that are protected using technologies such as access control or encryption

Likes 0	
Dislikes 0	
Response: Thank you for your comment. The term "storage locations" has been removed.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST strongly disagrees with the SDT's assertion that retention of "designated storage locations," is a hindrance to using third party / cloud services, and notes that the SAR for this project states the project will provide "…a secure path towards utilization of modern third-party data storage and analysis systems." The real roadblock here, for which solutions are already available, is encryption key management (see our response to Question 9). In addition, N&ST is concerned that one or more Regional Entities may or may not agree with the SDT's frequently repeated promise that managing access to BSCI storage locations will be accepted as a fully compliant equivalent to managing access to BCSI, and that Responsible Entities have the option of maintaining current practices. As a compromise, N&ST recommends the proposed CIP-004 changes be amended to state explicitly that Responsible Entities must manage access to one or more of: BCSI, designated electronic storage locations, and designated physical storage locations. This change would give entities the flexibility of maintaining or dropping "storage locations" or perhaps implementing a hybrid approach.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Based on the favorable vote from industry, the SDT determined the language of R6 accomplishes the objective to add flexibility for industry to leverage additional secure methods to protect BCSI; "designated storage locations," is one way to accomplish the objective and R6 as written does not precluded entities from using that approach. . It is up to each entity to determine how best to implement their programs to meet the requirements.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	
Comment	

The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, “Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.” The removal of, “storage locations” from R6 and its subparts, makes it difficult for the entities to comply, as the entities need to expand their searches for access control when providing compliance evidence.

We disagree with using, “provisioned access” as it is currently defined. The requirement to provide lists of personnel with “provisioned access” would also require entities to identify the locations of BCSI, and for auditors to make that link to the repository of BCSI, to determine which has been provisioned for access.

Similar to “Provisioned access” noun, simply stating “BCSI” will make it intangible where keeping “storage locations” will make the requirement and its subparts tangible. See Q1 comment.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at third-party off-prem (*cloud based*) locations.

Use language similar to that in CIP-011 that addresses cloud storage for the proposed CIP-004.

Recommend creating a NERC Glossary defined term for “Provisioned Access.”

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees the proposed changes retain the flexibility for storage locations to be used as one way to meet the objective.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
See comments in response to #9 below.	
Likes 0	

Dislikes 0	
Response: Please see the SDT's response to #9 below.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
NO. See WAPA and Indianca Comments.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Please see the SDT's response to WAPA.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC agrees that this approach provided entities with the flexibility to define their own internal procedures, which may include continuing to designate storage locations for BCSI to which individuals can have provisioned access. Provisioned access for those individuals can be authorized, verified, and revoked.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications which make the Requirement more objective-based.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Thomas Breene - WEC Energy Group, Inc. - 3	

Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern agrees as with EEI and industry that this approach provided entities with the needed flexibility to develop and define their own internal procedures of what constitutes storage for current and future use.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports this change.	

Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.	
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 NPCC Regional Standards Committee	

Answer	Yes
Document Name	
Comment	
If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
An organization should be able to define storage locations as well as decommission them, as long as appropriate controls are applied in both processes. The revised standard allows entities to apply controls at either the data level or storage level, without requiring either so long as data security is achieved.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	

Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Yes, this modification retains the flexibility for storage locations to be used as one way to meet the objective. However, absent clarifying language in the requirement regarding temporary and incidental access, the standard may inadvertently significantly expand the scope over the currently approved standard. This language is included in the Technical Rationale, but is not included in any enforceable language. It is recommended that additional clarification be added as outlined in the response to questions 1 and 2.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your comment. Please see the SDT's response to questions 1 and 2.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes

Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC RSC.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the approach provides entities with the needed flexibility to develop and define their own internal procedures regardless of whether they are using off-premise storage or simply maintaining backward compatibility with their legacy systems. However, we also recognize that the removal of the term "storage locations" does present challenges for entities trying to reconcile internal processes for legacy systems. For this reason, we recommend the SDT provide greater clarity through Implementation Guidance, to assist those entities with developing effective processes resulting from these changes. Specifically, the SDT should develop guidance that would be useful in understanding how to define storage locations as a method within registered entities' access management programs. Such guidance would be helpful to ensure backward compatibility.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of	

information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
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	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Black Hills does not find the distinction necessary. If consistent use of the language "obtain and use" then it should be evident that physical access to a computer, device, etc. does not constitute access to BCSI. The same logic that applies to a locked filing cabinet should apply to cyber access as well.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	No
Document Name	
Comment	

The IRC SRC observes that this approach appears to compensate for the removal of the concept of BCSI repositories. We suggest changing "physical access to physical BCSI" to "physical access to physical BCSI ***storage locations***" as "physical BCSI" limits the definition to the information itself (e.g. the drawings) and would not extend to include the protection of the storage location or repository as well (e.g. the drawer where the drawings are stored).	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Provisioned physical access to physical BCSI may very well be to a storage location.	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	
GRE disagrees that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets "obtain and use" condition and constitutes an access to BCSI. Recommendation: Adding "Physical access to unencrypted electronic BCSI" to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Although provisioned physical access to a physical location or storage device that contains electronic BCSI is not considered provisioned access to the electronic BCSI, entities should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011. If	

there are specific mechanisms available or feasible for provisioning electronic access to the unencrypted electronic BCSI, then this would be part of the R6 access management program.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to the ISO/RTO Council SRC.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy disagrees with the proposed changes, including a statement for both physical and electronic access only leads to further questions. CPS Energy propose defining what is considered Physical BCSI and Electronic BCSI as those terms are not defined by NERC – although should be understood Physical BSCI could be BSCI on printed medium, white board scribbles, photograph and electronic BCSI would be word docs, pdf, text file, digital photos – each person could define or scope the words physical and electronic in different ways.	
Likes 0	
Dislikes 0	

Response: Thank you for your comment. The significance of this is not so much about the format of the BCSI, but what access must be managed. As the currently enforceable requirement is written, it is unclear if an entity is required to manage physical access to electronic BCSI, an issue that is compounded when storing BCSI with a cloud service provider. The CMEP Practice Guide makes it clear that the intent is to manage electronic access to electronic BCSI, and physical access to physical BCSI, so the SDT spelled that out here. **The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.**	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
It is recommended that the SDT directly clarify the understanding that access to data or a tangible item that contains information does not equate to access to that information. The addition of such a clarification in the standard would simplify the understanding of the applicability of controls to the protection of BCSI.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your comment. The focus of the BCSI requirements in CIP-004 is managing individuals' access to BCSI where access can be provisioned, and the focus of CIP-011 is protecting the BCSI itself from unauthorized access no matter where the BCSI is located.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

See our comments around “provisioned access” in Q5 AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to Q5 and to ACES.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
See our comments around “provisioned access” in Q5	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to Q5.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	

In the measures for R6.1, suggested evidence includes “the justification of business need for the provisioned access.” However, similar requirement 4.1 states “authorize based on need” but does not call out the justification of business need in the measures. 6.1 and 4.1 should be consistent in measures.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Evidence should show compliance with all aspects of the requirements, hence the measure for justification of business need. The SDT felt it was out of scope to make changes to 4.1 that were not related to BCSI, but encourage entities to include justification of business need for that part as well.	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree that the physical access only applies to physical BCSI since the controlling access to unencrypted BCSI has not been addressed. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets “obtain and use” condition and constitutes an access to BCSI. We suggest adding “Physical access to unencrypted electronic BCSI” to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Although provisioned physical access to a physical location or storage device that contains electronic BCSI is not considered provisioned access to the electronic BCSI, entities should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011. If there are specific mechanisms available or feasible for provisioning electronic access to the unencrypted electronic BCSI, then this would be part of the R6 access management program.	

The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnte for a Standard.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language from the note to the parent requirement R6. In addition, the SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

"Physical BCSI" is not a defined term. AEP recommends SDT to either define "physical BCSI" or add further clarifications in Requirement 6. AEP recommends using the existing language, "*Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*" under 6.1.	
Likes 0	
Dislikes 0	
Response: Thank you for your commnet. The significance of this is not so much about the format of the BCSI, but what access must be managed. As the currently enforceable requirement is written, it is unclear if an entity is required to manage physical access to electronic BCSI, an issue that is compounded when storing BCSI with a cloud service provider. The CMEP Practice Guide makes it clear that the intent is to manage electronic access to electronic BCSI, and physical access to physical BCSI, so the SDT spelled that out here. **The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.**	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to Marty Hostler.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	

Answer	No
Document Name	
Comment	
We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets "obtain and use" condition and constitutes an access to BCSI. **Recommendation:** Adding "Physical access to unencrypted electronic BCSI" to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Although provisioned physical access to a physical location or storage device that contains electronic BCSI is not considered provisioned access to the electronic BCSI, entities should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011. If there are specific mechanisms available or feasible for provisioning electronic access to the unencrypted electronic BCSI, then this would be part of the R6 access management program.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
NO. Cloud services should be allowed. However, there is no need to make a distinction between electronic access and physical access.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis

Dislikes 0	
Response: Thank you for your comment. As the currently enforceable requirement is written, it is unclear if an entity is required to manage physical access to electronic BCSI, an issue that is compounded when storing BCSI with a cloud service provider. The CMEP Practice Guide makes it clear that the intent is to manage electronic access to electronic BCSI, and physical access to physical BCSI, so the SDT spelled that out here.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Further clarification should be made to CIP-004-X Part 4.1.2 and Part 6.1.2 to address the difference between physical access to a Physical Security Perimeter that may house BCSI versus physical access to a physical piece of hardware that houses BCSI. Where does the physical piece of hardware that houses BCSI need to be stored?	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy agrees the proposed changes enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". Duke Energy does not agree with, and recommends removing, "and the justification of business need for the provisioned access" as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees where they would likely cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Evidence should show compliance with all aspects of the requirements, hence the measure for justification of business need.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the distinctions made between "electronic access to electronic BCSI" and "physical access to physical BCSI".	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
"Physical BCSI" is not a defined term.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The significance of this is not so much about the format of the BCSI, but what access must be managed. As the currently enforceable requirement is written, it is unclear if an entity is required to manage physical access to electronic BCSI, an issue that is compounded when storing BCSI with a cloud service provider. The CMEP Practice Guide makes it clear that the intent is to manage electronic access to electronic BCSI, and physical access to physical BCSI, so the SDT spelled that out here. **The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.**	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments: For 6.2 and 6.3, OPG suggest to specify that the requirement is applicable to both physical and electronic provisioned access to BCSI similar to 6.1.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. 6.2 and 6.3 are about provisioned access to BCSI. Based on the favorable ballot results, the SDT does not plan to make any substantive changes.	

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Entergy does not oppose distinguishing electronic BCSI from physical BCSI; however, the change raises the question of how entities are to comply with 6.1.2. If someone prints out the ESP drawings on paper, must they then provide evidence of who has access to their office and how it was provisioned? Are we just going to expect that no hard copies of BCSI are created, or if so, they are only stored in a secure physical location with access controls? ***Specifying both electronic and/or physical access to BCSI will also mirror treatment of classified information – i.e. different protection strategies apply depending on the medium. It might be cleaner to just differentiate between electronic access and physical access. If you have physical access to a Cyber Asset, you still need to somehow get access to the electronic information stored on the physical***	

asset - electronic info protection strategies apply. If the physical asset is paper (or maybe removable media) then you may rely more heavily on physical protection strategies.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The significance of this is not so much about the format of the BCSI, but what access must be managed. As the currently enforceable requirement is written, it is unclear if an entity is required to manage physical access to electronic BCSI, an issue that is compounded when storing BCSI with a cloud service provider. The CMEP Practice Guide makes it clear that the intent is to manage electronic access to electronic BCSI, and physical access to physical BCSI, so the SDT spelled that out here. The focus of the BCSI requirements in CIP-004 is managing individuals' access to BCSI where access can be provisioned, whereas The focus of CIP-011 is protecting the BCSI itself from unauthorized access no matter where the BCSI is located. The CIP-004 R6 requirements are applicable when specific mechanisms are available or feasible for provisioning access to BCSI. Please see the Technical Rationale for further explanation.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached. Providing the definition of "provisioned access" within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for "Provisioned Access."	
Likes 0	
Dislikes 0	
Response: Thank youy for your comment. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part	

of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
N/A.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	

Comment	
ISO New England supports this change.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the distinction between "electronic access to electronic BCSI" and "physical access to physical BCSI."	

Likes 0	
Dislikes 0	
Response: Thank you for your support.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications and clarifications.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
By this change, can it be clarified that an entity's IT service provider server rooms (where electronic BCSI is hosted) does not fall under physical BCSI.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Although provisioned physical access to a physical location or storage device that contains electronic BCSI is not considered provisioned access to the electronic BCSI, entities should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011. If	

there are specific mechanisms available or feasible for provisioning electronic access to the unencrypted electronic BCSI, then this would be part of the R6 access management program.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC appreciates this distinction to enable the use of cloud service providers for entities that wish to use them and eliminate the interpretation that every possible encounter with BCSI cannot be access controlled in the way required by CIP-004, but would still be protected in another way under the entity's Information Protection Plan per CIP-011.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 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	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
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 NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	

5. The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	
Comment	

CIP-004-X R2, R3, and R4 discusses authorized access. A user is to be authorized prior to being provisioned. If the CIP-004-X R6 requirements focus on provisioned users there is a gap of users who may be authorized and not yet provisioned. The SDT should chose to define authorized access in place of or in conjunction with provisioned access.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. It is true that an individual is to be authorized prior to being provisioned access. This is the intent of R4 as well as R6. R2 (training) and R3 (personnel risk assessment) are prerequisites for authorization and provisioning of electronic access to applicable cyber systems and unescorted physical access into a PSP, but not for BCSI. It is also true that some individuals may be authorized for provisioned access to BCSI, but do not have provisioned access to BCSI at any given time. This is up to the entity to decide how best to implement.The SDT determined that the term "provisioned" does not need to be defined. Provision

or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
NO. NERC Terms need a definition which is to be used for both CIP and O&P standards. Else Registered Entities will be subject to Regional Entity auditor interpretations not vetted by industry.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Thank you for your comment. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
1. Based on WAPA's disagreement of the term"provisioned access" and given that the SDT has defined "access to BCSI" in R6, the term "provisioned access" should be removed due to the creation of an unintended security loophole (See our comments in Q1).	

2. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective "provisioned" adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

3. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

Likes 0	
Dislikes 0	

Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.

Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Marty Hostler.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The currently effective Requirement Part 4.1.3 of CIP-004-6 reads, "Access to designated storage locations, whether physical or electronic, for BES Cyber System Information." AEP suggests to use similar language from Part 4.1.3 as suggested in our response to Question #4 above. AEP recommends 6.1 use similar language to 4.1, i.e., "*Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information*"	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Please see the SDT"s response to Q3 comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	

Answer	No
Document Name	
Comment	
Dominion Energy is concerned the the SDT is attempting to define the term "provisioned access" in a footnote. Leaving a term open to interpretation across Standards is concerning and if a term is being used inconsistently it should be defined in the Glossary of Terms rather than through a footnte for a Standard.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6. Based on the comments received and ballot results, the SDT determined the language is sufficient as written. **The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.**	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
Given that SDT has defined the "access to BCSI" in R6, the provisioned access needs to be removed since it has a unintended security loophole (See our comments in Q1).	
Likes 0	
Dislikes 0	

Response: Thank you for your comment. Please see responses to comments in Q1.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Providing the definition of "provisioned access" within the Standard via the Note: within CIP-004 R6 Part 6.1 does not provide sufficient clarity to Industry. Tacoma Power suggests that it would be beneficial to create a NERC Glossary defined term for "Provisioned Access."	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6. Based on the comments received and ballot results, the SDT determined the language is sufficient as written. **The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.**	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

If “provisioned” is needed, then what is non-provisioned access? SRP does don’t think “provisioned” is necessary, but adding it does not cause much concern. Access might need to be a defined term rather than using notes even if broken down between O&P and CIP.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Although some may consider instances when an individual is merely given, views, or might see BCSI as “access to BCSI”, that is NOT “provisioned access to BCSI”. An example of this is when an individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. This “access” should be considered in the entity’s Information Protection Plan for CIP-011. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards. If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change.	

Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific: “Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI”. Due to the first sentence of the question, it is not possible to define “access” alone, thus definitions for various types of access could be defined such as BCSI Access in this case.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the “note” from 6.1 and moved the language to the parent requirement R6. Based on the comments received and ballot results, the SDT determined the language is sufficient as written.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
While we agree with the SDT usage of “provisioned” and the use of the “Note” to help clarify access, the “Note” does not reduce the audit risk to an Entity. The “Note” is purely there for explanation and is not a NERC accepted definition nor does it have to be accepted by an auditor. The fact this has to be explained or even noted shows the ongoing existing problem with the way “access” is used in the CIP standards. If a “Note” for “provisioned access” is needed to help scope “access”, then EVERY requirement with “access” in the CIP standards should have a “Note”. Defining “access” is not part of this SAR thus any modifications to “access” is out of the scope of the SAR and not a part of this change. Further the fact that the “Note” uses “is to be considered” is not binding to the requirement. It either is considered or not considered. The way the “Note” is written, access could or could not be “considered the result of the specific actions taken to provide an individual(s) the means to access BCSI”. If there was a way to make the “Note” binding, to be acceptable, the “Note” should be specific:	

"Provisioned access is the result of the specific actions taken to provide an individual(s) the means to access BCSI". Due to the first sentence of the question, it is not possible to define "access" alone, thus definitions for various types of access could be defined such as BCSI Access in this case. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6. Based on the comments received and ballot results, the SDT determined the language is sufficient as written. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term. Please see the SDT's response to ACES.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Tacoma Power.	

Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy suggests creating a NERC Glossary defined term for “Provisioned Access” instead of adding the Note: within CIP-004 R6 Part 6.1. Additionally, “obtain and use” should be included in the definition.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term “provisioned” does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	
a. Given that the SDT has defined “access to BCSI” in R6, and the term “provisioned access” should be removed due to the creation of an unintended security loophole (See our comments in Q1). b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured	

systems, implemented controls tasks and standardized programs on these terms. The adjective “provisioned” adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence. Recommendation: 1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. Please see responses to comments for Q1. **Regarding the security loophole, the SDT respectfully disagrees since the concept of provisioned access is the scoping mechanism for the requirement, not a loophole. Provisioned access provides the needed flexibility for a Responsible Entity to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located. While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program.**	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

N&ST notes that “provisioned” is not an adjective. Beyond that, “access” has already been given a contextual definition: “Obtain and use.” N&ST suggests the SDT maintain consistency with existing CIP-004 language and continue to require that Responsible Entities authorize access to BCSI and/or BCSI storage locations.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	

Comment	
MPC supports not defining “access” as a NERC glossary term, as this could be difficult and have unintended consequences for other standards. MPC agrees that the use of “provisioned” and the note adds enough context to clarify what kind of access the requirements are about.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Provisioned access’ in Part 6.3 doesn’t necessarily trigger the removal of accesses granted maliciously or inadvertently, and accepts a security and reliability risk that is mitigated in today’s language. The use of provisioned access in Part 6.1 (authorize) and 6.2 (verify) is fine. Consider “… ability to access BCSI…” instead of “…ability to use provisioned access…” for Part 6.3 only	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The trigger to remove access granted maliciously or inadvertently would be whenever it is found, such as during the verification required by 6.2. Part 6.3 is consistent with CIP-004-6 R5.3, with a termination action being the trigger. All of R6 is scoped to provisioned access, including revocation, as only that which is provisioned can be revoked. Please refer to the paragraph regarding R6 Part 6.3 in the Technical Rationale.	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the adjective "provisioned" and as noted in the comment for Question 1, will define what "provisioned" means to PG&E and following the definition in our implementation of the modifications.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes

Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Agree with the use of term provisioned. Would like the SDT to incorporate EEI comments as a non-substantive change during the final EEI review.	
Likes 0	
Dislikes 0	
Response: Thank you for your support and comment. Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the defining adjective of "provisioned" as the actions that may be taken to provide access to both electronic and physical BCSI. The "Note" further clarifies what possible specific actions may be considered as provisioned.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England supports the clarification in the "Note".	

Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Suggest reiterating the "Obtain and use" qualifier in the Main R6 requirement. This well better explain what "Access" really means.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6.	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree that the Note clarifies provisioned access. We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Part 4.1 requires a process to authorize access based on need. An entity may implement their program in such a way as to use the same authorization for both Part 4.1 and Part 6.1.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree that the Note clarifies provisioned access. We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1	
Likes 0	
Dislikes 0	

Response: Thank you for your comment. Part 4.1 requires a process to authorize access based on need. An entity may implement their program in such a way as to use the same authorization for both Part 4.1 and Part 6.1.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Considering the R6.1 'Note,' the SDT should further clarify "provisioned access" in the IG/Technical Rationale and specifically address the "underlay" (CSP environment) from the "overlay" (SaaS, IaaS, PaaS) where "provisioned access" to BCSI is given.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
From a technical standpoint, the addition of 'provisioned' provides clear delineation regarding the definition of 'access' in this context. Please reference the above comments in questions 1 and 2 regarding inclusion of clarifying language and guidance provided in the Technical Rationale within the standard. Additionally, it is recommended that the Note regarding provisioned access be moved to the main requirement in R6 where the term "provisioned access" is first used. This will also provide clarification that the note applies to all uses of the term within the requirement and not just part 6.1.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	

Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments: Please provide additional clarification why the use of term "provisioned" is limited to access to BCSI and not also in Requirement 4 and 5.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to NPCC Regional Standards Committee. CIP-004-X (and also CIP-004-6, the currently enforceable standard) R4 and R5 is/was already properly scoped to the kind of access to be authorized, verified, and revoked (i.e., electronic access to applicable cyber systems and unescorted physical access into a Physical Security Perimeter). Although this is also provisioned access, it is not necessary to add the qualifier to R4 and R5. However, it is necessary to include the word "provisioned" to scope the kind of access to BCSI the R6 requirements pertain to.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	

Dislikes 0	
Response: Please see the SDT's response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC has no concerns about adding "provisioned" to provide context, however, we are unsure if this helps clarify what constitutes access. Additional attempts to clarify "access" by the SDT may not be necessary. Individual entities have been successful in defining "access" for themselves and their programs whereby Attachment C and prior audit records can continue to support this approach.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Black Hills agrees with the decision, it should be evident that access is simply the ability to obtain and use, any further specifications beyond that should be an entity decision.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports not defining "Access" and agrees that providing a NERC glossary definition could have unintended consequences. EEI supports the decision to define "provisioned access" in the context of CIP-004 to be sufficient for the purposes of this standard but also recommends that this definition be elevated to the parent Requirement R6 given that "provision access" is used throughout this requirement. (See EEI comments to Question 1)	
Likes 0	
Dislikes 0	

Response: Thank you for your comment. The team removed the "note" from 6.1 and moved the language to the parent requirement R6.	
Donna Wood - Tri-State G and T Association, Inc. - 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	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 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	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to EEI.	

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

These proposed changes have not met the requirement of the SAR to prevent unauthorized access.

CIP-011 R1 Part 1.2, should be in alignment with CIP-004 R6 Part 6.1.

While detailed instructions are addressed in, “Measures” instead of in the “requirements.” Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in ‘Part 1.2 to broaden the focus on protecting and securely handling BCSI….’ in this current form it is contradictory with, ‘methods to protect’ in the Rationale, as their objectives are different.

Recommendation:

We suggest adding “prevent unauthorized access to BCSI” to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1:

“Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use.”

See the question to ‘broaden’ the focus of the language, and then the Technical Rationale says to be ‘explicit’…this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 & 1.4. This could result in a burden to industry here.

Likes 0	
Dislikes 0	
Response: Thank you for your comment. The requirement has been drafted in an objective based way with the intent of protecting BCSI regardless of the state (i.e., storage transit and use) it exists in. In this way, the SDT has clarified or broadened the intent by explicitly protecting BCSI in all states. **Please see the webinar from April 27, 2021 that explained CIP-004 being the access control and CIP-011 is the protective measures. The focus of the BCSI requirements in CIP-004 is managing individuals' access to BCSI where access can be provisioned, and the focus of CIP-011 is protecting the BCSI itself from unauthorized access no matter where the BCSI is located.**	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST agrees with the SDT's decision to drop proposed Requirement R1 Parts 1.3 and 1.4. However, we disagree with the proposed changes to Parts 1.1 and 1.2, as we believe the existing language adequately defines the required elements of an Information Protection Program.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Based on the comments received and ballot results, the SDT determined the language is sufficient as written.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
While detailed instructions are addressed in, “Measures” instead of in the “requirements.” Comparing with the previous draft; this version is less burdensome, and covers broader situations, and, it reduces the repeated way to present methods used in different states of transit, storage, and use. However, in ‘Part 1.2 to broaden the focus on protecting and securely handling BCSI….’ in this current form it is contradictory with, ‘methods to protect’ in the Rationale, as their objectives are different. NVE suggests adding “prevent unauthorized access to BCSI” to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1: “Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use.” See the question to ‘broaden’ the focus of the language, and then the Technical Rationale says to be ‘explicit’…this seems to be contradictory – this needs further investigation. See the new language in 1.2 as compared to the previous 1.3 & 1.4. This could result in a burden to industry here.

Likes 0	
Dislikes 0	
Response: Thank you for your comment. The team determined that the language is sufficient as is based on the favorable ballot body.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Texas RE is concerned that the proposed changes remove the concept of integrity, which is as equally important as the concept of confidentiality. The current approved language in Requirement Part 1.2 specifically supports the concept of integrity through the phrase “*storage, transit, and use.*” Texas RE asserts that such comprehensive language regarding BCSI storage, transit, and use – that is ensuring confidentiality and integrity – should continue to be included. Texas RE recommends adding “and integrity” after confidentiality in Requirement Part 1.2.

Additionally, Texas RE recommends the removal of "[i]mplementation of administrative methods" as an example of evidence for off-premise BCSI. If a Registered Entity intends to make use of third-party services for storing BCSI the Registered Entity is still responsible for ensuring the safety of the BCSI. A risk assessment or business agreement with the third-party vendor does not provide sufficient risk mitigation should the third-party vendor be compromised. Lastly, as mentioned in response to Question #2, Texas RE recommends adding bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2. Texas RE recommends the following language: 1.2.1 - Method(s) to limit the ability of unauthorized individuals from obtaining or using BCSI. 1.2.2 - Method(s) to limit the ability of unauthorized individuals from modifying BCSI without being detected. For those methods that use encryption, utilize an encryption key strength of at least 128 bits, in accordance with NIST. For those methods that use hashing, utilize a hash function with an output size of at least 256 bits, in accordance with NIST.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved. A single measure by itself does not tell an entity that they have met the entire requirement. The measures are suggested methods to assist. This measure is a good practice along with technical controls.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

The proposed simplification is useful with the exception of the verbiage added to Requirement R1.2. Specifically, the term to mitigate the risk of compromising confidentiality is overly broad and ambiguous and could result in subjective interpretation during audits. The technical rational states that this change was made to "reduce confusion" but instead it has only added ambiguity. The existing language does not hinder the objectives of this SDT in any manner. Keeping this language consistent with the approved version of the standard will prevent unnecessary modification of existing CIP-011 programs, especially for those entities who have no desire to use cloud-hosted solutions. As such, it is recommended that the language to R1.2 remain as follows: Method(s) to protect and securely handle BCSI, including storage, transit, and use.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your comment. The "mitigate risk" language takes into account the application of controls in a more targeted manner. This concept objectively addresses the removal of the previously proposed CIP 11 R1.3 and 1.4. This also aids in auditing and methodologies to perform a mitigation function to protect, as opposed to being a methodology to protect. This was used to aid auding / enforcement concerns within the SDT. The "storage, transit, and use" language was dropped to clarify that BCSI is protected comprehensively, regardless of being in "storage, transit, and use". This reduces confusion on interpreting, defining, and mapping controls to whatever state BCSI is in. This brings more consistency for Responsible Entity's and auditors alike. The "storage, transit, and use" language was maintained in the measures to aid in the clarity to the Responsible Entity that the concept of "storage, transit, and use" is still accounted for. BCSI, regardless of state or format, comprehensively requires protection.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	

In support of Tacoma Powers' comments. Attached.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Integrity is an important security objective for 'Real-time Assessment and Real-time monitoring data' and is address in CIP-012. However, this should not negate the need to ensure the integrity of BCSI remains a security objective as well as confidentiality.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No

Document Name	
Comment	
We agree with comments from Duke Energy.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Duke Energy.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power supports the inclusion of method(s) as opposed to procedure(s); however, the inclusion of the objective of "mitigate the risk of compromising confidentiality" does not follow the current language provided in CIP-012 on order to maintain Standards consistency. Therefore, Tacoma Power suggests the following alternative language: "Method(s) to protect and securely handle BCSI to mitigate the risks posed by unauthorized disclosure and unauthorized modification of BCSI." The inclusion of unauthorized modification supports the fact that entities rely on the integrity of their BCSI in many instances, and should provide protections for data integrity where there is a risk associated with data integrity.	

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	

Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.

Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	

Comment

We disagree with R1 Part 1.2 changes since these changes haven't resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI. Using "mitigate the risks.." is subjective resulting in no audit consistency since the NERC entities and auditors may have different ways to interpret it.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment	
We agree with the removal of language of “storage, security during transit, and use” from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The “storage, transit, and use” may be considered unnecessary or redundant due to the proposed requirement language being more comprehensive; the “storage transit, and use” language in the measures brings clarity and aids some Responsible Entity’s in the application, accounting, or evidence of controls that address BCSI.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
MidAmerican Energy agrees with removal of Parts 1.3 and 1.4. However, we are concerned with the lack of clarity of the language of Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI “becomes explicitly comprehensive.” This question refers to a “broadened” focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added to Technical Rationale regarding expectations of the requirement, including the difference between version 2 and the proposed version X. We agree with the removal of language of “storage, security during transit, and use” from the requirement. However, we do not see the need to mention this language again in the measures and ask that this language be removed.	
Likes 0	

Dislikes 0	

Response: Thank you for your comment. The "explicitly comprehensive" language in the Technical Rationale will be clarified. The "storage, transit, and use" may be considered unnecessary or redundant due to the proposed requirement language being more comprehensive; the "storage transit, and use" language in the measures brings clarity and aids some Responsible Entity's in the application, accounting, or evidence of controls that address BCSI.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy is concerned with the addition of "*to mitigate risks of compromising confidentiality*". This additional language seems to require that Registered Entities develop methodologies and processes to determine levels of risk. Furthermore, the term *mitigate risks* is very subjective and could be interpreted differently by the respective parties involved. This addition doesn't appear to address any risks or identified gaps. Please clarify the intent of the use of the language.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. The "mitigate risk" language takes into account the application of controls in a more targeted manner. This concept objectively addresses the removal of the previously proposed CIP 11 R1.3 and 1.4. This also aids in auditing and methodologies to perform a mitigation function to protect, as opposed to being a methodology to protect. This was used to aid auding / enforcement concerns within the SDT.

JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment
AEP supports the removal of Requirement R1 Parts 1.3 and 1.4, and the minor adjustment made to Requirement R1, Part 1.1. AEP has concerns that the adjustments made to Requirement R1, Part 1.2, made this requirement overly broad, especially considering the management of the off-premise BCSI. Specifically, AEP is concerned with the breadth and depth of L1 and L2 evidence that would be required to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise BCSI. Further, it is not clear what would constitute acceptable methodologies or procedures (self-audit, independent audits, SOC1/SOC2 reviews, etc.) for AEP to validate a third party's control environment (provided the third party cooperates with AEP's request) sufficient to demonstrate compliance and mitigating risks of compromising confidentiality associated with Requirement R1, Part 1.2 with regard to off-premise BCSI. Finally, it is not clear to what level AEP will need to document, monitor, and enforce controls implemented and administered by a third party who maintains AEP's BCSI off-premise. AEP is also concerned with any unintended consequences from the proposed language, as it could be interpreted to mean any vendor's use of BSCI, even if it is stored on AEP's systems, and not BSCI that is stored, transmitted, or used by a 3rd party vendors on their system(s).

Likes 0	
Dislikes 0	
Response: Thank you for your comment. The process that an entity would employ to assess risks associated with the management of the off-premise BCSI would determine the breadth and depth of L1 and L2 evidence that would be required to demonstrate compliance. The SDT was not intending to prescribe a one size fits all, but that an entity would adjust the risk assessment to the type of vendor service involved. If an entity believes that the risk assessment currently utilized for CIP-013 is an appropriate methodology focused on specific "risks" within the Responsible Entity's Information Protection Plan, then the SDT believes leveraging that would be an acceptable approach. Evidence demonstating self-audits, independent audits, SOC1/SOC2 reviews could be all be acceptable based upon how an Entity chooses to define their assessment methodology.	
William Steiner - Midwest Reliability Organization - 10	
Answer	No

Document Name	
Comment	
In CIP-011-X, Part 1.2, the proposed draft excludes risks related to data integrity. Omission of data integrity would require supplemental Practice Guides by the ERO Enterprise to determine what cloud environment risks are related to confidentiality vs. integrity. In practicality most data access risks overlap between those two legs of the CIA triad, and will be difficult or impossible to enforce some data risk scenarios with data confidentiality alone. Also, the mapping document 'Description and Change Justification' indicates that the focus for CIP-011-X Part 1.2 was intended to be broader, but the change appears to be narrower than existing language. One or the other must be in error, but we are not sure which.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to Marty Hostler.	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
We do not agree with R1 Part 1.2 changes since these changes haven't resolved the goal of SAR that is to prevent unauthorized access to BCSI while in transit, storage, and in use. CIP-011 requirements should be in alignment with CIP-004 R6 Part 6.1 to ensure only authorized personnel can possess BCSI. Recommendations: We suggest adding "prevent unauthorized access to BCSI" to R1 Part 1.2 so that it is in alignment with CIP-004 R6.1: "Method(s) to protect and securely handle BCSI Information to prevent unauthorized access to BCSI, including storage, transit, and use."	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDT believes that the current proposed language within R1 Part 1.2 does not preclude an Entity from needing to prevent the unauthorized access to BCSI while in transit, storage, and in use.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
NO. We agree with removing CIP-011XX R1 Parts 1.3 & 1.4.	

We do not agree with adjusting Part 1.2.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Thank you for your comment.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
While more clear than the previously proposed CIP-011-3, the provided measures for CIP-011-X Part 1.2 it states, implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements). Business agreements and vendor service risk assessments does lead to confusion with CIP-013.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The SDTs intent by including "Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements)" within the Measures of R1 Part 1.2 was acknowledge that Entities could leverage CIP-013 risk assessment processes for the storage and analysis of BCSI by third party vendors.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy generally agrees with the proposed changes of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality.

Duke Energy has concerns with the wording of measures for R1.2. 'on-premise BCSI' and 'off-premise BCSI' are open to interperetation. Is it the intent that a third party managed BCSI repository that is implemented on 'on-premise' servers not be subject to the 'off-premise' measures? Can a risk assessment determine the actual controls, physical, technical or administrative, needed?

Duke Energy recommends that for third party (or 'off-premise') managed or hosted storage, a risk assessment for physical, technical and administrative controls be performed and mitigating controls be implemented as determined.

Likes 0	
Dislikes 0	

Response: Thank you for your comments. The SDT agrees with your approach that each Entity should perform a risk assessment for physical, technical and administrative controls and implement mitigating controls for each third party service provider that handles BCSI. The type (depth) of assessment and resulting mitigating controls would depend upon the type and location of the servies provided. Additionally, an Entity may need to rely upon a 3rd party independent audit report, SOC1/SOC2 reviews, etc. to achieve that objective.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees with removal of Parts 1.3 and 1.4. However, we suggest additional clarity of the language in Part 1.2. The CIP-011-X Technical Rationale states that methods to protect BCSI "becomes explicitly comprehensive." This question refers to a "broadened" focus, but the requirement does not clearly explain the broadened focus and comprehensive expectations. We request additional information be added

to the Technical Rationale regarding the expectations of this requirement, including the difference between Draft 2 and the proposed Draft 3 version. EEI agrees with protection of BCSI itself over the physical location in which BCSI is stored. We also support the removal of the language "storage, security during transit, and use" from this requirement. However, the language within the measure should also be removed. Furthermore, EEI does not support the use of the term "in use," because this language is not necessary or auditable.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
This draft is much more favorable than the previous. It's more open ended and the "confidentiality" statement aligns better with the spirit of what BCSI protection programs should aim to achieve.	
Likes 0	
Dislikes 0	
Response: Thank you for you support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	

Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC supports the SDT's removal of parts 1.3 and 1.4 as retaining them in CIP-011 would have added another CIP standard to the scope of supply chain requirements. We view this as a good change.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC Regional Standards Committee.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	

Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to EEI.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree with this simplification.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with this simplification.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes

Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	

ISO New England agrees with this simplification.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the deletion of CIP-011-X Requirement R1 Parts 1.3 and 1.4 and simplifying Parts 1.1 and 1.2. The SDT has made it clear the protection of BCSI itself is what is addressed here over where the BCSI is actually stored.	

Likes 0	
Dislikes 0	
Response: Thank you for your support.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E does not believe there is any double jeopardy between the proposed modifications to CIP-011-X and CIP-013.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
MPC agrees with the proposed changes and believes that CIP-011 requires protection of BCSI no matter where it is located. To do this, entities must conduct assessments to understand what BCSI they have, where it can be found, how it transmits, what is done with it, and understand how confidentiality could be compromised at any of these times and locations in order to implement appropriate controls to protect it. While MPC appreciates the reminder in the measures to consider BCSI that is located on-premises and off-premises, using these terms here may be confusing. MPC suggests including additional information in Technical Rationale or Implementation Guidance instead.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
In the Measures for R1.2, change "on-premise" to "on-premises” and “off-premise” to “off-premises”.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT will make this non-substantive change.	

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see SDT's response to Marty Hostler.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the extension of the 24-months implementation plan provided the CIP-004 R6.1 requirement to document justification of the need for authorization is eliminated.	
Likes 0	
Dislikes 0	

Response: Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC agrees with this approach.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the 24-month implementation plan and the ability for early adoption.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the 24-month timeline. It will allow enough time to reach implementation.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to EEI.	
John Galloway - ISO New England, Inc. - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
ISO New England agrees with aligning timelines.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	

Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon has elected to align with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We agree with aligning timelines.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree with aligning timelines.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	Yes
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Yes, 24 months is sufficient and aligning the changes with the Project 2016-02 SDT modifications will improve the efficiency and cost-effectiveness of the adjustments required to comply with these modifications.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your support.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to NPCC RSC.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The IRC SRC acknowledges the SDT for incorporating our prior suggestion for added flexibility.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	

Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposal to extend the implementation plan to 24-months because changes will be necessary to align processes and training with the new requirements for both entities planning to utilize cloud services as well as those not planning to do so. EEI also supports the option for early adoption.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 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	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
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	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dan Bamber - ATCO Electric - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	

Response: Please see the SDT's response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

***8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach*?**	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Unknown fiscal impacts without a cost impact analysis and further clarifications. PAC has strong concerns regarding the broadened and "explicitly comprehensive" expectations for CIP-011-X R1.2, which could result in significant impacts that are not cost-effective. Standards should not be approved by until each SDT develop a detailed cost estimate. There is no information to determine if the modifications are a cost-effective approach	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST's selection of "No" reflects our belief that currently proposed changes should be amended.	

Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Unknown at this time. The broadened approach to BCSI protections in CIP-011, could lead to potential high costs to an Entity.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP still holds to our comments from last time - the cost to implement will grow quickly with unclear requirements that lead to Responsible Entity concerns of proper interpretation. We would not say these are cost-effective at this time	
Likes 0	
Dislikes 0	

Response: Thank you for your comment.	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	No
Document Name	
Comment	
MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
At this time PG&E does not have information to determine if the modifications are a cost-effective approach.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	

Comment	
MidAmerican Energy is concerned with broadened and “explicitly comprehensive” expectations for CIP-011-X R1.2, which could result in a costly approach.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Please reference Marty Hostler's comments. Thanks.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to Marty Hostler.	
Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	

The SDT has not provided a cost estimate. Consequently, we have no idea if the proposal is cost effective. Standards should not be approved by Industry until each Standard Drafting Team develops a detailed cost estimate (capital and maintenance). This means including internal controls, more staff, management/board approval, budgetting, revising all Internal Compliance Documents to account for the new standard or modifications, etc. All these changes end up costing real people, our customer, they certainly would not blindly tell the STD I just want that product and don't care what the cost is.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response: Thank you for your comment.	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends removing “and the justification of business need for the provisioned access” as a measure in CIP-004 R6.1. Managers must be able to authorize access to a large number of employees without need to cut and paste a blanket justification for each person or group. All that should be required is documented authorization and removal along with the record of authorized individuals. The act of authorization should be considered sufficient that a business need for access exists. There is no risk reduction in documenting this justification, but there is significant overhead in adding such functionality to existing authorization tools.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment.	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	Yes
Document Name	
Comment	
The proposed changes appear to be backwards compatible, allowing entities to quickly adapt current compliance programs to incorporate the changes and are a substantial improvement over the last draft.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
None.	
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	
Southern agrees that the proposed changes are cost effective. There may be additional costs in the future for the use of different technology or applications but would be budgeted for any planned upgrades.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	

We think this is a cost effective way to address the issue.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Any changes made result in a cost to industry.	
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	Yes
Document Name	
Comment	
See comments in response to #9 below.	
Likes 0	

Dislikes 0	
Response: Please see the SDT's response to #9 below.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dan Bamber - ATCO Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	
Answer	
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
N/A.	
Likes 0	

Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Unfortunately we wouldnt be able to properly answer this question at this time.	
Likes 0	
Dislikes 0	
Response	

9. Please provide any additional comments for the SDT to consider, if desired.
Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment
Tri-State Generation and Transmission appreciates the time and effort given to this project and agrees with the revisions/changes.

Likes 0	
Dislikes 0	

Response: Thank you for your support.
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	
Document Name	

Comment
No additional comments.

Likes 0	
Dislikes 0	

Response
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	
Comment	
The proposed language is too ambigious and obligates entities to protect BCSI in any form, even though beyond its control. Should BCSI be shared with NERC/FERC, the proposed standard would require registered entities to extend their access management to include the copy of that information held by NERC/FERC. Subsequent requirements in CIP-011 would require reviews of access rights associated with that copy. The language should be re-scoped to focus on management of access to designated repositories, instead of the information itself.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Based on the favorable ballot results, the SDT does not foresee this as an issue.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	
Document Name	
Comment	
The CIP-004-X and CIP-011-X proposal is more favorable than the previous CIP-004-7 and CIP-011-3 approach of moving access management of BCSI from CIP-004 and adding it to CIP-011.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	

Marty Hostler - Northern California Power Agency - 3,4,5,6	
Answer	
Document Name	
Comment	
none.	
Likes 1	Northern California Power Agency, 6, Sismaet Dennis
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

The SDT should work to simplify but clarify the standards. Years down the road auditors make interpretations and companies need to be clear what is required. Secondly the SDT should look at ISO and NIST standards for guidance. Per our comments in question 1, WAPA recommends changing “provisioned access” to “access to BCSI” for whole R6 and its parts as suggested here:

“Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

- For changes to R6 Part 6.2:

Verify at least once every 15 calendar months that all individuals with access to BCSI:

6.2.1. have an Is authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, as determined by the Responsible Entity.

- For changes to R6 Part 6.3:

For termination actions, remove the individual's ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action."

As we suggested in Q1, changing from "provisioned access to BCSI" to "access to BCSI" provides the clarity and flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. Therefore, the SDT does not see the need to remove "provisioned" from the language.

Dennis Sismaet - Northern California Power Agency - 6

Answer	
Document Name	

Comment

Please reference Marty Hostler's comments. Thanks.

Likes 0	

Dislikes 0	
Response: Please see the SDT's response to Marty Hostler.	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	
Document Name	
Comment	
The SSRG wants to thank the drafting team for their time and efforts on this project.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	
Document Name	
Comment	
No further comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

CIP-004-X R6 and CIP-011-X R1 have different applicability. In the Draft 3 language, BCSI pertaining to medium impact BCS without ERC must be protected (CIP-011-X R1), but access to this BCSI need not be controlled (CIP-004-X R6). Without mandated access controls, the entity will be left to determine what is an effective protection to BCSI pertaining to medium impact BCS without ERC. The SDT should consider revisiting the differences in applicability between CIP-004-X R6 and CIP-011-X R1. Since this issue is beyond the scope of the 2019-02 SAR, please add this concern to the list of SAR items for the next revision of CIP-004.

The Background sections of CIP-004-x and CIP-011-X should be moved to their respective Technical Rationale documents.

CIP-004-X Implementation Guidance: 1) Implementation Guidance for R2 states that “a single training program for all individuals needing to be trained is acceptable” which is in conflict with the language in R2, “appropriate to individual roles, functions, or responsibilities.” 2)

Page numbers for R6 are incorrect. 3) Appendix 1 should be moved to the Technical Rationale document as it does not fit the requirements for Implementation Guidance. Implementation Plan: The “Early Adoption” paragraph should make it clear that all of the updated Requirements must be adopted at the same time. An entity should not be permitted to early-adopt only parts of the revised Standards.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The team will provide your proposed edits to NERC staff for future project consideration. The team did not make edits to Requirement R2. Regarding early adoption, this is a discussion you will need to hold with your Regional Entity upon considering early adoption.	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	
Document Name	
Comment	
OKGE supports comments provided by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT’s response to EEI.	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	

Comment
MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4. While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue**.**

Likes 0	
Dislikes 0	

Response: Thank you for yoru comment. Based on the favorable ballot results, the SDT does not plan to make any substantive changes.

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	

Comment
PG&E thanks the SDT for the effort in making the modifications objective based that will allow PG&E to implement them to fit our environment.

Likes 0	
Dislikes 0	

Response: Thank you for your support.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	
Document Name	
Comment	
MidAmerican Energy continues to have concern with the revised text of CIP-004-X R6.2. Please add a statement to the CIP-004-X Technical Rationale document: The review expected in CIP-004-X R6.2 is expected to be the same as CIP-004-6 R4.4. While we are generally supportive of the changes to CIP-004, we are concerned about creating a new separate requirement for BCSI authorization, revocation and review. This creates the potential for non compliance of multiple requirements for a single situation, such as revocation of accesses for a termination. We ask the SDT to consider making changes that will reconcile this issue.	
Likes 0	
Dislikes 0	
Response: Thank you for yoru comment. Based on the favorable ballot results, the SDT does not plan to make any substantive changes.	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	
We support EEI comments.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	

Bruce Reimer - Manitoba Hydro - 1	
Answer	
Document Name	
Comment	

Resulting from our comments in Q1, we suggest changing “provisioned access” to “access to BCSI” for whole R6 and its parts.

Recommendations:

Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

For changes to R6 Part 6.2:

Verify at least once every 15 calendar months that all individuals with access to BCSI:

6.2.1. have an authorization record;

6.2.2. Is still need the access to BCSI to perform their current work functions, as determined by the Responsible Entity.

For changes to R6 Part 6.3:

For termination actions, remove the individual’s ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

As we suggested in Q1, changing from “provisioned access to BCSI” to “access to BCSI” would provide the clarity and the flexibility for authorizing, verifying, and revoking access” to BCSI using various approaches including BCSI repository level or BCSI file level protection, which make the R6 backwards compatible.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. Therefore, the SDT does not foresee changes needed.	
David Hathaway - WEC Energy Group, Inc. - 6	
Answer	
Document Name	
Comment	
Support comments made by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	
Document Name	
Comment	
Supportive of EEI comments on this project.	

Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
Tacoma Power supports the objective of the Project 2019-02 SAR, which includes providing a path to allow the use of modern third-party data storage and analysis systems. While the use of third-party data storage may be enabled to a degree with these modifications, the use of third-party analysis systems is likely not. Any managed security provider's solution would likely be considered an EACMS based on the current definition, which carries a host of CIP Requirements, not the least of which are found in CIP-004, which would preclude the use of these services in almost every case. Tacoma Power suggests modification of the EACMS NERC Glossary definition to split off access control from access monitoring, which then would allow for requirement applicability based on risk for access control systems versus access monitoring systems.	
Likes 1	Snohomish County PUD No. 1, 3, Chaney Holly
Dislikes 0	
Response: Thank you for your comment. The EACMS modification is outside the scope of this projects SAR.	

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
PNM Resources appreciates the work of the SDT and the opportunity to provide feedback.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
CIP-004 R6.2, in the Measures, suggest removing "Verification that provisioned access is appropriate based on need" – the need is confirmed by the authorization of access. Also, the measure should align with the requirement 6.2.2, which does not say "based on need"	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Evidence should show compliance with all aspects of the requirements, hence the measure for justification of business need.	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	
Document Name	
Comment	
Request clarification on Part 6.2's Measures. Will auditing / enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example." We look forward to seeing the final combined version of this update and the virtualization update.	
Likes 0	
Dislikes 0	
Response: Evidence should show compliance with all aspects of the requirements, and that measure is one example of the several items of evidence that would do so.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	
Document Name	
Comment	
Request clarification on Part 6.2's Measures. Will auditing/enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example." We look forward to seeing the final combined version of this update and the virtualization update.	
Likes 0	
Dislikes 0	
Response: Evidence should show compliance with all aspects of the requirements, and that measure is one example of the several items of evidence that would do so.	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
We would like to thank the SDT for allowing us to comment.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response: Thank you for your support.	
Jennifer Flandermeyer - Jennifer Flandermeyer On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Jennifer Flandermeyer	

Answer	
Document Name	
Comment	
Evergy supports and endorses the comments filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
These changes are viewed as an overall improvement to the requirements around BCSI in CIP-004 and CIP-011. However, it would be more effective if these requirements were integrated into the existing framework of CIP-004 R4 and R5 rather than creating a new requirement R6. As it is now proposed, entities will need to recognize that authorizations are now covered in R4 and R6, periodic access reviews now exist in R4 and R6, and revocations are required in both R5 and R6. While the requirements are outlined reasonably, this separation creates a new burden on readability of the standards and training new staff regarding compliance expectations.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response: Thank you for your comments. The SDT does support an Entities ability to leverage third-party audit reports to assess the risk and controls for to demonstrate compliance with CIP-011-X R1 Part 1.2. The Implementation Guidance will reflect this approach. ion of business need. The SDT felt it was out of scope to make changes to 4.1 that were not related to BCSI, but encourage entities to include justification of business need for that part as well.	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned by now explicitly including the concept of confidentiality in CIP-011, Part 1.2, the SDT has inadvertently removed the concept of integrity from the scope of the proposed CIP-011. As noted in Texas RE's response to Question 6, the current approved language in CIP-011 that states "*storage, transit, and use*" in Part 1.2 supports the concept of integrity. Texas RE recommends adding "and integrity" after confidentiality in Requirement Part 1.2. Texas RE also recommends including a bright line criteria for determining usability of BCSI to CIP-011 Requirement Part 1.2 should be established to ensure consistent application of the standard.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. The integrity concern is beyond the scope of this SAR and it is not the intent of the SDT to include Integrity requirements/objectives in this draft. Furthermore, the security objective of the BCSI requirements is to protect BES Cyber Systems. If the confidentiality of the BCSI is protected, then the risk of BCSI being misused by a bad actor and that bad actor impacting BES Cyber Systems is also protected and the security goal has been achieved.	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
CPS Energy does not have any additional comments at this time.	

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT hereby incorporates the comments filed by the ISO/RTO Council Standards Review Committee. In addition the ISO/RTO Council comments, ERCOT offers the following additional comments. First, with respect to Reliability Standard CIP-004-x, Requirement 6, Parts 6.1 and 6.2, the concept of roles should be allowed to be consistent with Requirement R4. This could be addressed in the requirement language or accompanying measure. If this is not permitted, ERCOT would appreciate an explanation explain why in the consideration of comments. Second, ERCOT believes the SDT should address the ability to use third-party audit reports in verifying the controls for third parties. Similarly, ERCOT would appreciate an explanation whether this is allowed or not, and why.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT does support an Entities ability to leverage third-party audit reports to assess the risk and controls for to demonstrate compliance with CIP-011-X R1 Part 1.2. The Implementation Guidance will reflect this approach. ion of business need. The SDT felt it was out of scope to make changes to 4.1 that were not related to BCSI, but encourage entities to include justification of business need for that part as well.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	

Comment
OPG supports NPCC Regional Standards Committee's comments, and has the following additional comments: CIP 004-X 4.1 requires entity to have a "process"; where 6.1 requires the entity to authorize but a "process" is not required. Both requirements seem to have similar intent with 4.1 applying to the Applicable System and 6.1 applying to BSCI. Please provide clarification whether the discrepancy is intentional.

Likes 0	
Dislikes 0	

Response: Please see the SDT's response to NPCC RSC. Both requirements do have similar intent in that authorization is required prior to provisioning access, and the discrepancy is intentional.

Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	
Document Name	

Comment
1. Resulting from our comments in Q1, we suggest changing "provisioned access" to "access to BCSI" for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3: • For changes to R6 Part 6.2: Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. have an Is authorization record; 6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity.

• For changes to R6 Part 6.3: For termination actions, remove the individual's ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action. We believe "access to BCSI" provides the flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible. 2. The SDT may consider cleaning up the language to potentially the following language: R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information - that collectively include each of the applicable requirement parts in CIP004-X Table R6 – Access Management for BES Cyber System Information. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning] Revised Language Recommendations 6.1 Prior to authorization (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Electronic access to electronic BCSI; and 6.1.2. Physical access to physical BCSI. Note: Access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights) 6.2 Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. Have a current authorization record; and 6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. Based on the comments received and ballot results, the SDT determined the language is sufficient as written.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Alliant Energy supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2019-02 BCSI Access Management (Draft 3)	
Answer	
Document Name	2019-02_Unofficial_Comment_Form_BCSI Access Management_IRC SRC_05-10-21_FINAL.docx
Comment	
CIP-011-X, Part 1.2, Measures: The IRC SRC recommends the SDT clarify that encrypted information, also known as cipher text, is not BCSI. Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, <delete cipher,> electronic key management); or	

Note: MISO abstains from the response to item 9.	
Likes 0	
Dislikes 0	
Response: Thank you for your comment. Based on the favorable votes, the SDT does not plan to make substatitive changes.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response: Please see the SDT's response to EEI.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
N&ST has two additional comments, and associated recommendations, to respectfully offer. The first comment is that in our opinion, the proposed changes do not address one of the project's stated goals, which is "…to clarify the protections expected when utilizing third-party solutions (e.g., cloud services)." N&ST is aware of the SDT's desire to avoid writing overly	

prescriptive requirements, such as was done in the first set of proposed revisions to CIP-011, but we nonetheless believe the issue of who is creating, and has the potential ability to use, authentication credentials such as encryption keys must be addressed in the Standards in one or more Requirements (vs. in "Measures" or guidance documents). We are aware of one Responsible Entity that was found by a Regional Entity audit team to be out of compliance with CIP-004 for storing BCSI in the cloud and relying on the cloud service provider's default encryption. Simply dropping "storage locations" from CIP-004 would not, by itself, have helped the Responsible Entity avoid this problem. N&ST therefore recommends the following or similar language be added to either CIP-004 or CIP-011:

"The Responsible Entity shall ensure that all individuals, including those affiliated with third parties such as vendors and cloud service providers, who possess the means to obtain and use BCSI that is protected by one or more electronic and/or physical access controls (login credentials, unlock passwords, encryption keys, cardkeys, brass keys, etc.) have been authorized in accordance with CIP-004 requirements."

N&ST's second comment is that we are concerned there is insufficient clarity with regards to what distinguishes "provisioning" from "sharing." During the recent SDT webinar, a member of the SDT gave listeners a good example: (paraphrasing) Person A, who has been provisioned access to a file cabinet and has a key, opens it and gives a BCSI document to Person B, who has not been authorized for access to the file cabinet and cannot open it. Person A has shared BCSI with Person B. The SDT has already created a contextual definition of "access to BCSI." N&ST recommends that a similar contextual definition of "sharing" be added to either CIP-004 or CIP-011, working off the example the SDT itself created.

Likes 0	
Dislikes 0	

Response: Thank you for your comment. According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use

the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI. **CIP-004 focuses on protection for provisioned accses and does not in any way state sharing.**
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment
Recommend creating a NERC Glossary defined term for “Provisioned Access.” “Physical BCSI” is not a defined term. “Storage Locations” is no longer explicitly stated. The language should be re-scoped to focus on management of access to designated repositories We appreciate all the time and effort given to this project to develop these revisions/changes. However, if you are approving a new set of Standards, we recommend that the Technical Guidance is also published at the same time. The excessive delay between these publications, is causing industry confusion. The VSL – this is excessively severe (Proposed VSLs are based on a single violation and not cumulative violations.) Recommend: Use the same language as previously in R4:

R4: Operations Planning and Same Day Operations – VRF Medium The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) Authorize happens *prior* to provisioning access R6.R1 – See Note: The SDT is relying HEAVILY on the CMEP guide for definition parameters, and not the STD language. Clarify BOTH CIP-004 & CIP-011 requirements relating to managing access and protecting BCSI.	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. Based on the comments received and ballot results, the SDT determined the language is sufficient as written.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI is concerned with having two separate requirements within CIP-004-X that address access removal. (See Requirement R5 (BCS) and R6 (BCSI) While we understand the intent and reasons for this change, often access is provided to individuals for both BCS and BCSI and any failure in the termination of access in these cases will result in two violations for the same error. We recommend that this issue be reconciled**.**	
Likes 0	
Dislikes 0	
Response: Thank you for your comments. The SDT determined that the term "provisioned" does not need to be defined. Provision or provisioned access is a well-known term among technical subject matter experts who provision access or deprovision access as a part	

of their job. This is an industry-proven and accepted term that aligns with security best practices and industry frameworks, which is best maintained as a non-defined term.	
Jose Avendano Mora - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
See comments submitted by Edison Electric Institute	
Likes 0	
Dislikes 0	
Response: Please see the SDT"s response to EEI.	
Thomas Standifur - Austin Energy - 1,3,4,5,6	
Answer	
Document Name	TPWR_2019-02_Unofficial_Comment_Form_2021-05-10.docx20210504-17090-hsevrj.docx
Comment	
Likes 0	
Dislikes 0	
Response	

Comments received from Basin Electric Power Cooperative

1. *The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

   ☐ Yes
   ☒ No

   Comments: The term "provisioned access" adds another undefined term to the NERC standards and doesn't provide a clear path to regulatory off-prem or cloud data center services as proposed in the SAR. The only methods to control access to off-prem (cloud) BCSI is either by 1) encrypting BCSI or 2) purchasing services which allow the entity to manage the off-prem authentication systems – thereby preventing 3rd party systems administrators or others from compromising entity BCSI stored in cloud data centers. Option 2 is highly unlikely.

   a. "Provisioned access" creates a security loophole whereas entities only require authorization for a provisioned access. For example, if access to BCSI is not provisioned, no authorization to BCSI is required. This does not meet the goal of SAR for controlling access to BCSI. Given the R6 definition whereas "access to BCSI" occurs when an individual has both "the ability to obtain and use BCSI," we recommend changing "provisioned access" to "access to BCSI".
   b. The term "unless already authorized according to Part 4.1" should be removed. Why? Because having authorized access to CIP Cyber Assets does not preclude the authorization for having access to BCSI.
   c. The use of "provisioned, provision or provisioning" of "access," regardless of tense, would require entities to be audited to, maintain, and provide documented lists of people and the "provisioned" configurations of entity BES Cyber System Information repositories in order to "verify" the "authorization" of such provisioned access. The Measures section highlights this expectation where evidence may include individual records, or lists of whom is authorized. To achieve this evidence, entities would need to provide evidence of systems accounts of on-premises or off premises system repositories of BCSI. Cloud providers will not provide such lists of personnel who have administrative level access to cloud BCSI server repositories and entities will be unable to verify what 3rd party off-prem systems administrators have access to BCSI, yet entities will be asked to provide this information for an entire audit cycle

d. The current language requiring entities to 1) identify repositories and 2) authorize access based on need can also work for 3rd party off-prem or cloud locations without requiring lists of personnel or configurations of systems accounts for repositories of BCSI. (see recommendations)

Recommendations:

1. Focus only on addressing electronic and physical access to BCSI in off-prem or cloud situations.
2. Consider the following language for R6 Part 6.1:

   Authorize access to BCSI based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances. Access to BCSI includes:

   6.1.1. Electronic access to electronic BCSI;

   6.1.2 Physical access to physical BCSI;

   6.1.3 Physical access to unencrypted electronic BCSI (See our comments in Q4).
3. Consider using the perspective of language in CIP-011 " to prevent unauthorized access to BES Cyber System Information." This allows entities to determine the risk and methods to protect BCSI
4. Consider using "authentication systems or encryption of BCSI" for personnel accessing electronic BCSI on cloud prem providers locations.

2. *The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

a. We agree to adding "obtain and use" language to clarify what constitutes an access to BCSI, but disagree to the use of "provisioned access". After clarifying the access to BCSI, the language "provisioned" should be removed since it has a security flaw and requires extensive records from repositories of BCSI (See our comments in Q1).

Recommendations:

1. Only use the term "access" as recommended in Q1

3. *The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

a. We agree to retaining the flexibility for storage locations to be used as one way to meet the objective of SAR, but disagree to using "provisioned access" (See our comments regarding "provisioned access" in Q1).

b. The requirement to provide lists of personnel with "provisioned access" would also require entities to identify the locations of BCSI and by auditors whom are required to make the link between the repository of BCSI which has been provisioned for access.

Recommendation:

Retain the current language and focus on auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

4. *To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

We disagree that the physical access only applies to physical BCSI since controlling access to unencrypted BCSI has not been addressed but will be required for 3rd party off-prem (cloud) repositories. The physical access to Cyber Assets is a fast avenue to owning the unencrypted electronic BCSI it contains, which meets "obtain and use" condition and constitutes an access to BCSI.

Recommendation:

Adding "Physical access to unencrypted electronic BCSI" to R6 Part 6.1.3 (See our suggested R6 Part 6.1 changes in Q1).

5. *The SDT considered industry comments about defining the word "access". "Access" is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define "access" in the NERC Glossary of Terms. Instead, the SDT used the adjective "provisioned" to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective "provisioned" in conjunction with the "Note" clarifies what "provisioned access" is? If not, please provide the basis for your disagreement and an alternate proposal.*

☐ Yes
☒ No

Comments:

a. Given that the SDT has defined "access to BCSI" in R6, and the term "provisioned access" should be removed due to the creation of an unintended security loophole (See our comments in Q1).
b. Access, which occurs in CIP standards language, whether it is electronic and/or logical access, physical access, unescorted physical access, remote access, or interactive remote access is clearly understood, has been widely adopted by industry and regulators, and has been subject to hundreds of audits across all regions for the past 14 years. Entities have developed internal documentation, configured systems, implemented controls tasks and standardized programs on these terms. The adjective "provisioned" adds further terms, requires changes and is of little value regarding the actions required of entities and the output deliverables or evidence.

Recommendation:

1. Revise the language to focus on access to BCSI and the auditable methods to protect BCSI at 3rd party off-prem (cloud) locations.

6. *In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.*

☒ Yes
☐ No

Comments: does not explain Prior language in the Rationale for Modifications to Requirement R1, Part 1.2 "By removing this language, methods to protect BCSI becomes explicitly comprehensive."

7. *The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal.*

☒ Yes
☐ No

Comments:

8. *In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?*

☒ Yes
☐ No

Comments:

9. *Please provide any additional comments for the SDT to consider, if desired.*

Comments:

1. Resulting from our comments in Q1, we suggest changing "provisioned access" to "access to BCSI" for whole R6 and its parts. Except our suggested changes to R6 Part 6.1, we also have the following recommendations for R6 Part 6.2 and 6.3:

- For changes to R6 Part 6.2:

  Verify at least once every 15 calendar months that all individuals with access to BCSI:
  6.2.1. have an Is authorization record;
  6.2.2. Is still need the access to BCSI to perform their current work functions, appropriate based on need, as determined by the Responsible Entity.

- For changes to R6 Part 6.3:

  For termination actions, remove the individual's ability to access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

We believe "access to BCSI" provides the flexibility for authorizing, verifying, and revoking access" to BCSI using various approaches including BCSI repositories and BCSI files, which make the R6 backwards compatible.

2. **The SDT may consider cleaning up the language to potentially the following language:**
   R6. Each Responsible Entity shall implement an access management program(s) to authorize, verify, and revoke access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-X Table R6 – Access Management for BES Cyber System Information - that collectively include each of the applicable requirement parts in CIP004-X Table R6 – Access Management for BES Cyber System Information.

[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]

Part	Revised Language Recommendations
6.1	Prior to authorization (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Electronic access to electronic BCSI; and

	6.1.2. Physical access to physical BCSI. Note: Access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights)
6.2	Verify at least once every 15 calendar months that all individuals with access to BCSI: 6.2.1. Have a current authorization record; and 6.2.2. A justification for authorization to perform their current work functions, as determined by the Responsible Entity.

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

REMINDER

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Additional Ballots and Non-binding Polls Open through May 10, 2021

Now Available

Additional ballots and non-binding polls for the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, May 10, 2021** for the following:

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection
- Implementation Plan

Due to projects 2019-02 BES Cyber System Information Access Management (BCSI) and 2016-02 Modification to CIP Standards (2016-02) both modifying CIP-004 and CIP-011, an "-X" has been added in place of the version numbers for BCSI and a "-Y" for the 2016-02 standards. Once both projects are completed, they will be combined together into one version, prior to submission to the NERC Board.

Balloting

Ballot pool members can log into the Standards Balloting and Commenting System (SBS) and submit votes.

Note: Votes cast in the previous ballots will not carry over to the additional ballots. It is the responsibility of the registered voter in the ballot pool(s) to vote again.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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 ballot results will be announced and posted on the project page. 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, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-02 BCSI Observer List” in the Description Box.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Formal Comment Period Open through May 10, 2021

Now Available

A 45-day formal comment period is open through **8 p.m. Eastern, Monday, May 10, 2021** for the following:

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection
- Implementation Plan

Due to projects 2019-02 BES Cyber System Information Access Management (BCSI) and 2016-02 Modification to CIP Standards (2016-02) both modifying CIP-004 and CIP-011, an "-X" has been added in place of the version numbers for BCSI and a "-Y" for the 2016-02 standards. Once both projects are completed, they will be combined together with one version, prior to submission to the NERC Board.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted April 30 – May 10, 2021.

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

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2019-02 BCSI Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

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
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 AB 3 ST
Voting Start Date: 4/30/2021 12:01:00 AM
Voting End Date: 5/10/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 231
Total Ballot Pool: 274
Quorum: 84.31
Quorum Established Date: 5/10/2021 4:48:09 PM
Weighted Segment Value: 83.75

Actions

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	77	1	40	0.8	10	0.2	2	9	16
Segment: 2	2	0.2	1	0.1	1	0.1	0	0	0
Segment: 3	60	1	40	0.833	8	0.167	0	4	8
Segment: 4	17	1	11	1	0	0	0	2	4
Segment: 5	67	1	43	0.827	9	0.173	0	7	8
Segment: 6	44	1	23	0.697	10	0.303	0	4	7
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.6	6	0.6	0	0	0	0	0
Totals:	274	5.8	164	4.857	38	0.943	2	27	43

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A

1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
3	Puget Sound Energy, Inc.	Nicolas Pacholski		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A

5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	No Comment Submitted
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

1	Manitoba Hydro	Bruce Reimer	Negative	Comments Submitted
1	Long Island Power Authority	Isidoro Behar	None	N/A
5	Manitoba Hydro	Yuguang Xiao	Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith	None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas	None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood	Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter	None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
		Aaron		

3	FirstEnergy - FirstEnergy Corporation	Ghodooshim		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson		Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason	Stefanie Burke	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	No Comment Submitted
			Denise		

6	Imperial Irrigation District	Diana Torres	Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
		Donna			

6	Great River Energy	Stephenson	None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil	Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson	None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan	Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead	Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender	Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer	Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal	None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield	Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert	Affirmative	N/A
5	New York Power Authority	Zahid Qayyum	Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Affirmative	N/A
3	Exelon	Kinte Whitehead	Affirmative	N/A
5	Exelon	Cynthia Lee	Affirmative	N/A
6	Exelon	Becky Webb	Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	Affirmative	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel	Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney	Affirmative	N/A
	Public Utility District No. 1 of Snohomish			

4	County	John Martinsen		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
6	AEP	JT Kuehne		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Paul McCurley		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris		None	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
1	Duke Energy	Laura Lee		Negative	Comments Submitted
					Comments

1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Submitted
5	East Kentucky Power Cooperative	David Meade	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 AB 3 ST
Voting Start Date: 4/30/2021 12:01:00 AM
Voting End Date: 5/10/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 231
Total Ballot Pool: 273
Quorum: 84.62
Quorum Established Date: 5/10/2021 4:43:25 PM
Weighted Segment Value: 81.39

Actions

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	77	1	39	0.796	10	0.204	2	10	16
Segment: 2	2	0.2	2	0.2	0	0	0	0	0
Segment: 3	59	1	38	0.826	8	0.174	0	5	8
Segment: 4	17	1	10	1	0	0	0	3	4
Segment: 5	67	1	43	0.811	10	0.189	0	7	7
Segment: 6	44	1	22	0.688	10	0.313	0	5	7
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.6	4	0.4	2	0.2	0	0	0
Totals:	273	5.8	158	4.721	40	1.079	2	31	42

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A

1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
3	Puget Sound Energy, Inc.	Nicolas Pacholski		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	No Comment Submitted
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

3	Lakeland Electric	Steve Marshall	None	N/A
3	Georgia System Operations Corporation	Scott McGough	Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer	Negative	Comments Submitted
1	Long Island Power Authority	Isidoro Behar	None	N/A
5	Manitoba Hydro	Yuguang Xiao	Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith	None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas	None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood	Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik	Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A

3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson		Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	No Comment Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A

1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A

1	NextEra Energy - Florida Power and Light Co.	Mike ONeil	Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden	Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson	None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan	Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead	Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender	Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer	Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal	None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield	Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert	Affirmative	N/A
5	New York Power Authority	Zahid Qayyum	Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver	Affirmative	N/A
1	Exelon	Daniel Gacek	Affirmative	N/A
3	Exelon	Kinte Whitehead	Affirmative	N/A
5	Exelon	Cynthia Lee	Affirmative	N/A
6	Exelon	Becky Webb	Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	Affirmative	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon	Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt	Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro	Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Affirmative	N/A

6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
6	AEP	JT Kuehne		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Paul McCurley		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris		None	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
5	East Kentucky Power Cooperative	David Meade		Negative	Third-Party Comments

3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Comment: View Comment Results
Ballot Name: 2019-02 BES Cyber System Information Access Management Implementation Plan AB 3 OT
Voting Start Date: 4/30/2021 12:01:00 AM
Voting End Date: 5/10/2021 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 225
Total Ballot Pool: 269
Quorum: 83.64
Quorum Established Date: 5/10/2021 5:04:33 PM
Weighted Segment Value: 92.51

Actions

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	76	1	43	0.915	4	0.085	1	12	16
Segment: 2	2	0.2	2	0.2	0	0	0	0	0
Segment: 3	58	1	41	0.891	5	0.109	0	5	7
Segment: 4	17	1	10	1	0	0	0	3	4
Segment: 5	65	1	43	0.896	5	0.104	0	9	8
Segment: 6	44	1	27	0.871	4	0.129	0	4	9
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.5	5	0.5	0	0	0	1	0
Totals:	269	5.7	171	5.273	18	0.427	1	35	44

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Nicolas Pacholski		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A

4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A

1	Tri-State G and T Association, Inc.	Donna Wood	Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza	Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock	None	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A

5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	No Comment Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A

1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		None	N/A

1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
5	Enel Green Power	Mat Bunch		Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	None	N/A
6	AEP	JT Kuehne		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A

5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Affirmative	N/A
6	Lakeland Electric	Paul Shipps	Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Abstain	N/A
6	Duke Energy	Greg Cecil	Affirmative	N/A
5	Duke Energy	Dale Goodwine	Affirmative	N/A
3	Duke Energy	Lee Schuster	Affirmative	N/A
4	National Rural Electric Cooperative Association	Paul McCurley	None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright	None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Third-Party Comments
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Third-Party Comments
1	Duke Energy	Laura Lee	Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Affirmative	N/A
5	East Kentucky Power Cooperative	David Meade	Negative	Third-Party Comments
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-004-7 Non-Binding Poll AB 3 NB
Voting Start Date: 4/30/2021 12:01:00 AM
Voting End Date: 5/10/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 213
Total Ballot Pool: 257
Quorum: 82.88
Quorum Established Date: 5/10/2021 4:58:31 PM
Weighted Segment Value: 84.57

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	70	1	35	0.833	7	0.167	14	14
Segment: 2	2	0.2	1	0.1	1	0.1	0	0
Segment: 3	59	1	34	0.872	5	0.128	11	9
Segment: 4	14	1	10	1	0	0	2	2
Segment: 5	62	1	34	0.85	6	0.15	13	9
Segment: 6	43	1	17	0.739	6	0.261	10	10
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.6	6	0.6	0	0	0	0
Totals:	257	5.8	137	4.994	25	0.806	51	44

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Abstain	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A

5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Nicolas Pacholski		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A

1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott		Affirmative	N/A

		Gill		
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett	Affirmative	N/A
		Salvatore		

1	New York Power Authority	Spagnolo		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason	Stefanie Burke	Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A

3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

1	Exelon	Daniel Gacek	Affirmative	N/A
3	Exelon	Kinte Whitehead	Affirmative	N/A
5	Exelon	Cynthia Lee	Affirmative	N/A
6	Exelon	Becky Webb	Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	Affirmative	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang	Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Affirmative	N/A
5	AEP	Thomas Foltz	Abstain	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Abstain	N/A
6	AEP	JT Kuehne	Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski	Affirmative	N/A
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes	Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson	Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Abstain	N/A
6	Lakeland Electric	Paul Shipps	Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Affirmative	N/A
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A

5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Negative	Comments Submitted
5	East Kentucky Power Cooperative	David Meade	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 Non-Binding Poll AB 3 NB
Voting Start Date: 4/30/2021 12:01:00 AM
Voting End Date: 5/10/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 214
Total Ballot Pool: 258
Quorum: 82.95
Quorum Established Date: 5/10/2021 5:03:23 PM
Weighted Segment Value: 82.61

Actions

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	70	1	35	0.833	7	0.167	14	14
Segment: 2	2	0.2	2	0.2	0	0	0	0
Segment: 3	59	1	33	0.846	6	0.154	11	9
Segment: 4	14	1	10	1	0	0	2	2
Segment: 5	63	1	32	0.821	7	0.179	15	9
Segment: 6	43	1	17	0.739	6	0.261	10	10
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment:	0	0	0	0	0	0	0	0

9								
Segment: 10	6	0.6	4	0.4	2	0.2	0	0
Totals:	258	5.8	133	4.839	28	0.961	53	44

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Abstain	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A

5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Nicolas Pacholski		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A

1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		None	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
1	Lakeland Electric	Larry Watt	None	N/A
5	Lakeland Electric	Becky Rinier	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	Comments Submitted
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
5	Tennessee Valley Authority	M Lee Thomas	Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman	Abstain	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett	Affirmative	N/A

1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise	Affirmative	N/A

			Sanchez		
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Abstain	N/A
6	Santee Cooper	Marty Watson		Abstain	N/A
3	Santee Cooper	James Poston		Abstain	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

1	Exelon	Daniel Gacek	Affirmative	N/A
3	Exelon	Kinte Whitehead	Affirmative	N/A
5	Exelon	Cynthia Lee	Affirmative	N/A
6	Exelon	Becky Webb	Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel	Affirmative	N/A
5	Enel Green Power	Mat Bunch	Abstain	N/A
4	CMS Energy - Consumers Energy Company	Aric Root	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long	None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner	Affirmative	N/A
5	Great River Energy	Jacalynn Bentz	Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis	Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen	Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang	Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads	Affirmative	N/A
5	AEP	Thomas Foltz	Abstain	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol	Abstain	N/A
6	AEP	JT Kuehne	Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski	Affirmative	N/A
3	Austin Energy	W. Dwayne Preston	Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes	Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson	Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax	Abstain	N/A
3	AEP	Kent Feliks	Abstain	N/A
6	Lakeland Electric	Paul Shipps	Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne	Negative	Comments Submitted
6	Duke Energy	Greg Cecil	Negative	Comments Submitted
5	Duke Energy	Dale Goodwine	Negative	Comments Submitted
3	Duke Energy	Lee Schuster	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup	None	N/A

3	Arkansas Electric Cooperative Corporation	Mark Gann	None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris	None	N/A
1	East Kentucky Power Cooperative	Amber Skillern	Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods	Negative	Comments Submitted
1	Duke Energy	Laura Lee	Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray	Affirmative	N/A
5	East Kentucky Power Cooperative	David Meade	Negative	Comments Submitted
3	Wabash Valley Power Association	Susan Sosbe	None	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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: All BES Facilities.

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

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-X.

6. **Background:** Standard CIP-004 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 common subject matter of the requirements.

   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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

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

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

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. EACMS; and 2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their	For termination actions, revoke the	An example of evidence may include,

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: • EACMS	individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The 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.

2. Table of Compliance Elements

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

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

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
~~10-day final ballot~~	~~May 2021~~
Board adoption	November 2021

A. Introduction

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

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

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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: All BES Facilities.

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

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-X.

6. **Background:** Standard CIP-004 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 common subject matter of the requirements.

   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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

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

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

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

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

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

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. EACMS; and 2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

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

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their	For termination actions, revoke the	An example of evidence may include,

CIP-004-X Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: • EACMS	individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI. ~~Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).~~	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The 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.

2. Table of Compliance Elements

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

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

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

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity ~~has~~ did not implement~~ed~~ one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2-11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

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

2. **Number:** CIP-004-X~~6~~

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each ~~Special Protection System (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**~~

4.1.6.4.1.5. Reliability Coordinator

4.1.7.4.1.6. Transmission Operator

4.1.8.4.1.7. 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 ~~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-004-X6:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-004-X~~6~~.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-X~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-X~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-X6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-X~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-X6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-X~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-X~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-X6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	High Impact BES Cyber Systems and their associated: • EACMS; and • PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • EACMS; and • PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: • A dated listing of authorizations for BES Cyber System information; • Any privileges associated with the authorizations; and • Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-X6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-X~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-X6 Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: EACMS; and PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: EACMS; and PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
5.34	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-X6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.45	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-X Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-X Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

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, 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 the NERC Reliability Standards in their respective jurisdictions.

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 Eapplicable 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 EThe applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible EThe 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 EnforceAssessment Programcesses:

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.

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-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity ~~has~~ did not implement~~ed~~ one or more documented program(s) for access management that includes a process to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information~~	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented~~	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is~~	authorize electronic access~~,~~ or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			storage locations, privileges were incorrect or unnecessary. (4.4)	processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.43) OR The Responsible Entity has implemented one or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, or unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4~~5~~) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the	reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar~~	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances. (5.54)	day following the effective date and time of the termination action. (5.3)		
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-X~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

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

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

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

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

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

Requirement R2:

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven-year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this~~

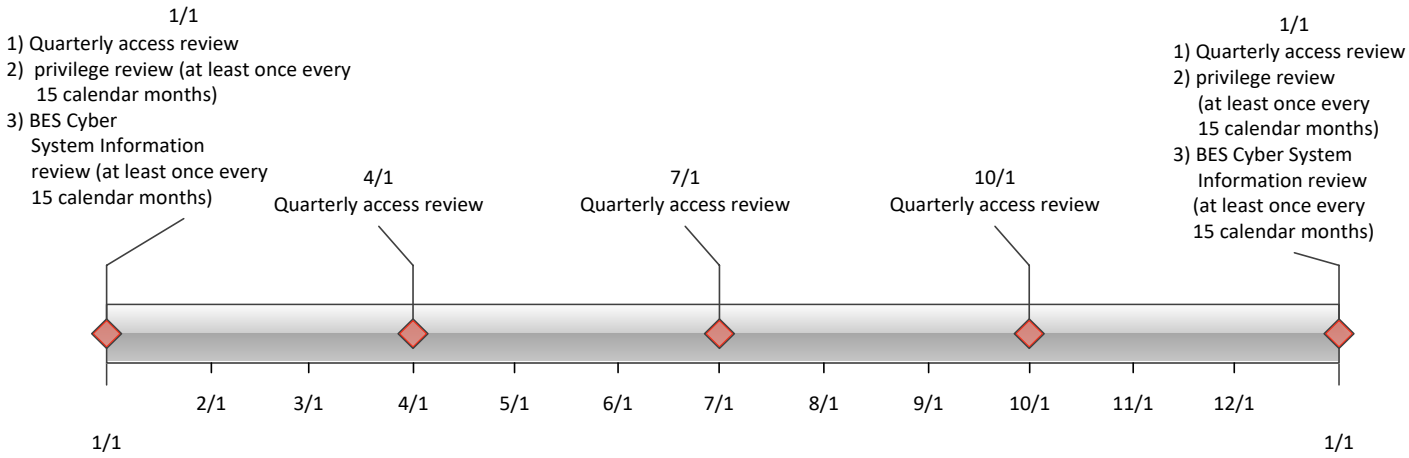
~~could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.~~

~~Requirement R4:~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

~~Rationale:~~

~~During 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:~~

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

~~Rationale for Requirement R2:~~

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

~~Rationale for Requirement R3:~~

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

~~Rationale for Requirement R4:~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~**hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.**~~

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

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

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

2. **Number:** CIP-004-7

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

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

   4.1.2.2. Each 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. 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: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-7.

6. **Background:** Standard CIP-004 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 common subject matter of the requirements.

   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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		Cyber Assets, including Transient Cyber Assets, and with Removable Media.	
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	their associated: 1. EACMS; and 2. PACS		
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS		Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and Logs or other demonstration showing such persons no longer have access.
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High Impact BES Cyber Systems and their	For termination actions, revoke the	An example of evidence may include,

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: • EACMS	individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 mandatory and enforceable Reliability Standards in their respective jurisdictions.

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 applicable 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:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The 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.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within	2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did	retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs)	not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk	and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR

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

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)	authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has implemented one or more process(es) to remove the ability for	The Responsible Entity has not implemented any documented program(s) for access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	and Operations Planning		user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of	revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	the next calendar day following the predetermined date. (5.2)	the next calendar day following the predetermined date. (5.2)	access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6 – September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2-11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-7~~6~~

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

4. Applicability:

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

4.1.1. Balancing Authority

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

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

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

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

4.1.2.2. Each ~~Special Protection System (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.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~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 ~~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-004-7~~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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-004-7~~6~~.

6. Background:

Standard CIP-004 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 common subject matter of the requirements.

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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.

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

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

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter~~; and~~ ~~4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.~~	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter~~, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information~~.

CIP-004-76 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS; and~~ ~~PACS~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~EACMS; and~~ ~~PACS~~	~~For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.~~	~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.~~
5.3~~4~~	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part~~s~~ 5.1 ~~or 5.3~~) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4~~5~~	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-7 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

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, 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 ~~the NERC~~ Reliability Standards in their respective jurisdictions.

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 E~~applicable 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 E~~The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- ~~If a Responsible E~~The 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 Enforce~~Assess~~ment Program~~cesses~~:

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.

~~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-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has did not implemented one or more documented program(s) for access management that includes a process to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information~~	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented~~	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is~~	authorize electronic access~~,~~ or unescorted physical access~~, or access to the designated storage locations where BES Cyber System Information is located~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~storage locations, privileges were incorrect or unnecessary. (4.4)~~	~~processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~	~~correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~	specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) ~~OR~~ ~~The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Same Day Operations and Operations Planning	Medium	~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~ ~~OR~~ The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.43) OR The Responsible Entity has implemented one or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access~~,~~ or unescorted physical access~~, or BES Cyber System Information storage locations~~. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.45) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the	reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar~~	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)~~	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances. (5.54)	~~day following the effective date and time of the termination action. (5.3)~~		
R6	Same Day Operations and Operations Planning	Medium	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2)	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-76)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

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 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
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-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	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.
6	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.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

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

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

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

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

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

Requirement R2:

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

~~One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.~~

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

~~Requirement R3:~~

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

~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this~~

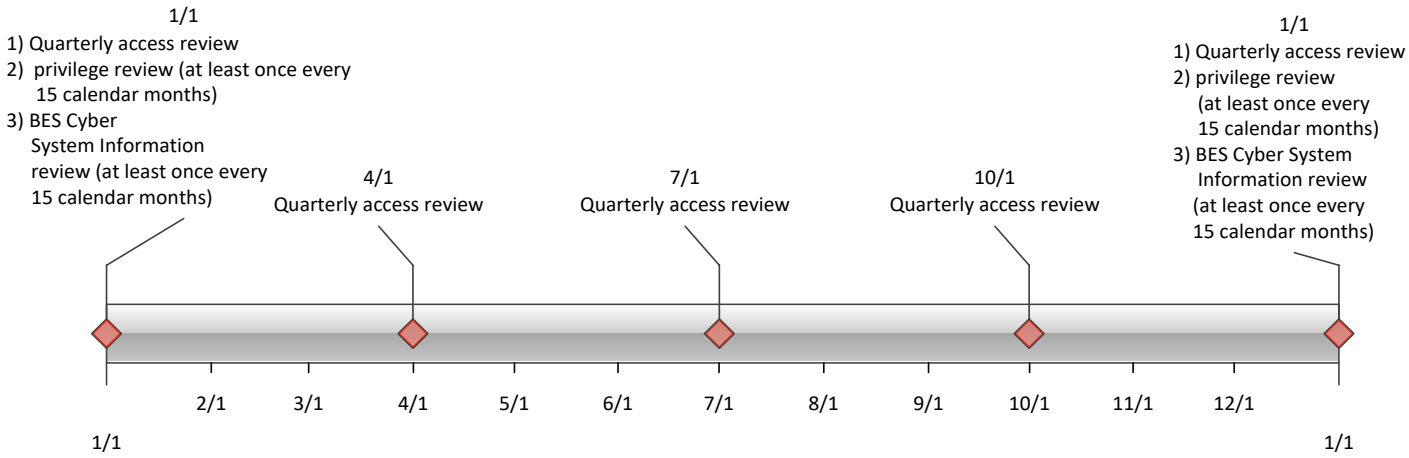
~~could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.~~

~~Requirement R4:~~

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

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

~~The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the~~



~~need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.~~

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

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

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

~~Requirement R5:~~

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

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

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

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

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

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

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

~~Rationale:~~

~~During 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:~~

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

~~Rationale for Requirement R2:~~

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

~~Rationale for Requirement R3:~~

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

~~Rationale for Requirement R4:~~

~~To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.~~

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

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

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

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

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

~~Rationale for Requirement R5:~~

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

~~In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the~~

~~**hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.**~~

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

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-X

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-X:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-011-X.

6. **Background:** Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 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 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 applicable 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:

- The 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-X Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
~~10-day final ballot~~	~~May 2021~~
Board adoption	November 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-X

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-X:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-011-X.

6. **Background:** Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-X Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 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 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 applicable 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:

- The 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-X Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2-11,2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-X~~2~~

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-X~~2~~:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-X~~2~~.

6. Background:

Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-X Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-X~~2~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-X~~2~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X~~2~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify ~~information that meets the definition of BES Cyber sytem Information~~ BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify ~~BES Cyber System Information~~ BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~ BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify ~~BES Cyber System Information~~ BCSI; or • ~~Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.~~ • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-~~2~~X Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	~~Procedure(s) for protecting and~~Method(s) to protect and securely handl~~e~~ing ~~BES Cyber System Information~~BCSI~~, including storage, transit, and use~~to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use ~~of BES Cyber System information~~; or • Records indicating that ~~BES Cyber System Information~~ BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical

CIP-011-X~~2~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain ~~BES Cyber System Information~~ BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyebr System Information~~ BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-X~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain ~~BES Cyber System Information~~BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~ BCSI prior to the disposal of an applicable Cyber Asset.

B. 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, 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 ~~the NERC~~ 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 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 applicable 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~~.~~:

~~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~~ The applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~Responsible~~ applicable ~~E~~entity is found non-compliant, it shall keep information related to the noncompliance 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 Process~~ 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~X2~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2) ~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented ~~a~~ one or more ~~BES Cyber System Information~~ BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-X~~2~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.1)	include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-X~~2~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2 – 11, 2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-3

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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 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:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-3:

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-002-5.1a identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-011-3.

6. **Background:** Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "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 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 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 applicable 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:

- The 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 #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-3 Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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	March 22, 2019
SAR posted for comment	March 28, 2019 – April 26, 2019
45-day formal comment period with ballot	December 20, 2019 – February 3, 2020
45-day formal comment period with ballot	August 6– September 21, 2020
45-day formal comment period with ballot	March 25 – May 10, 2021
10-day final ballot	June 2-11,2021

Anticipated Actions	Date
Board adoption	November 2021

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-3~~2~~

3. Purpose: To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against 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**~~**4.1.5 Reliability Coordinator**

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~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 ~~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-011-3~~2~~:

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-002-5.1a identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-011-3~~2~~.

6. Background:

Standard CIP-011 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 "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a 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 information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify ~~information that meets the definition of BES Cyber sytem Information~~ BCSI.	Examples of acceptable evidence may include, but are not limited to, the following: • Documented method(s) to identify ~~BES Cyber System Information~~ BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~ BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify ~~BES Cyber System Information~~ BCSI; or • ~~Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.~~ • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	~~Procedure(s) for protecting and~~Method(s) to protect and securely handl~~e~~ing ~~BES Cyber System Information~~BCSI~~, including storage, transit, and use~~to mitigate risks of compromising confidentiality.	Examples of acceptable evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling BCSI, which include topics such as storage, security during transit, and use ~~of BES Cyber System information~~; or • Records indicating that ~~BES Cyber System Information~~ BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical

CIP-011-~~2~~3 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~3~~2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [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-011-~~3~~2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	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	Prior to the release for reuse of applicable Cyber Assets that contain ~~BES Cyber System Information~~ BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the Cyber Asset data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyebr System Information~~ BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-~~2~~3 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	Prior to the disposal of applicable Cyber Assets that contain ~~BES Cyber System Information~~BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence may include, but are not limited to, the following: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~ BCSI prior to the disposal of an applicable Cyber Asset.

B. 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, 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 ~~the NERC~~ 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 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 applicable 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~~.~~:

~~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~~ The applicable ~~E~~entity shall retain evidence of each requirement in this standard for three calendar years.
- If a ~~Responsible~~ applicable ~~E~~entity is found non-compliant, it shall keep information related to the noncompliance 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 Process~~ 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.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2) ~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented ~~a~~ one or more ~~BES Cyber System Information~~ BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented processes but did not	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.1)	include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~ BCSI from the BES Cyber Asset. (2.2)	processes for applicable requirement parts in CIP-011-3~~2~~ Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection 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-011-1. (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-011-2. Docket No. RM15-14-000	

3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

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:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~Requirement R2:~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of Project 2019-02 BES Cyber System Information (BCSI) Access Management is to clarify the CIP requirements related to both managing access and securing BCSI. This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

[1] See subject standards for additional information on Distribution Providers subject to the standards.

General Considerations

The 24-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011; and
- Administrative overhead to review their program.

The 24-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide Electric Reliability Organization (ERO) and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-X – Cyber Security - Personnel & Training

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 twenty-four (24) 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 twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-X – Cyber Security - Information Protection

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 twenty-four (24) 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 twenty-four (24) 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

Responsible Entities shall initially comply with the periodic requirements in the CIP-004-X and CIP-011-X within the periodic timeframes of their last performance under the CIP-004-6 and CIP-011-2.

Compliance Dates for Early Adoption of Revised CIP Standards

A Responsible Entity may elect to comply with the requirements in CIP-004-X and CIP-011-X following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-X and CIP-011-X Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-X in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-X in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2019-02 BES Cyber System Information Access Management Reliability Standard CIP-004 and CIP-011

Applicable Standard(s)

- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-011-3 – Cyber Security - Information Protection

Requested Retirement(s)

- CIP-004-6 – Cyber Security - Personnel & Training
- CIP-011-2 – Cyber Security - Information Protection

Prerequisite Standard(s)

- None

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

The purpose of Project 2019-02 BES Cyber System Information (BCSI) Access Management is to clarify the CIP requirements related to both managing access and securing BCSI. This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

[1] See subject standards for additional information on Distribution Providers subject to the standards.

General Considerations

The 24-month period provides Responsible Entities with sufficient time to come into compliance with new and revised Requirements, including taking steps to:

- Implement electronic technical mechanisms to mitigate the risk of unauthorized access to BCSI when Responsible Entities elect to use vendor services;
- Establish and/or modify vendor relationships to ensure compliance with the updated CIP-004 and CIP-011; and
- Administrative overhead to review their program.

The 24-month implementation period will allow budgetary cycles for Responsible Entities to allocate the proper amount of resources to support implementation of the updated CIP-004 and CIP-011. In addition, the implementation period will provide Electric Reliability Organization (ERO) and Responsible Entities flexibility in case of unforeseen circumstances or events and afford the opportunity for feedback to be provided to the ERO and Responsible Entities through various communication vehicles within industry (e.g., NERC Reliability Standards Technical Committee, North American Transmission Form), which will encourage more ownership and commitment by Responsible Entities to adhere to the updated CIP-004 and CIP-011.

Effective Date

CIP-004-7 – Cyber Security - Personnel & Training

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 twenty-four (24) 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 twenty-four (24) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

CIP-011-3 – Cyber Security - Information Protection

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 twenty-four (24) 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 twenty-four (24) 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

Responsible Entities shall initially comply with the periodic requirements in the CIP-004-7 and CIP-011-3 within the periodic timeframes of their last performance under the CIP-004-6 and CIP-011-2.

Compliance Dates for Early Adoption of Revised CIP Standards

A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.

Retirement Date

CIP-004-6 – Cyber Security - Personnel & Training

Reliability Standard CIP-004-6 shall be retired immediately prior to the effective date of CIP-004-7 in the particular jurisdiction in which the revised standard is becoming effective.

CIP-011-2 – Cyber Security - Information Protection

Reliability Standard CIP-011-2 shall be retired immediately prior to the effective date of CIP-011-3 in the particular jurisdiction in which the revised standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

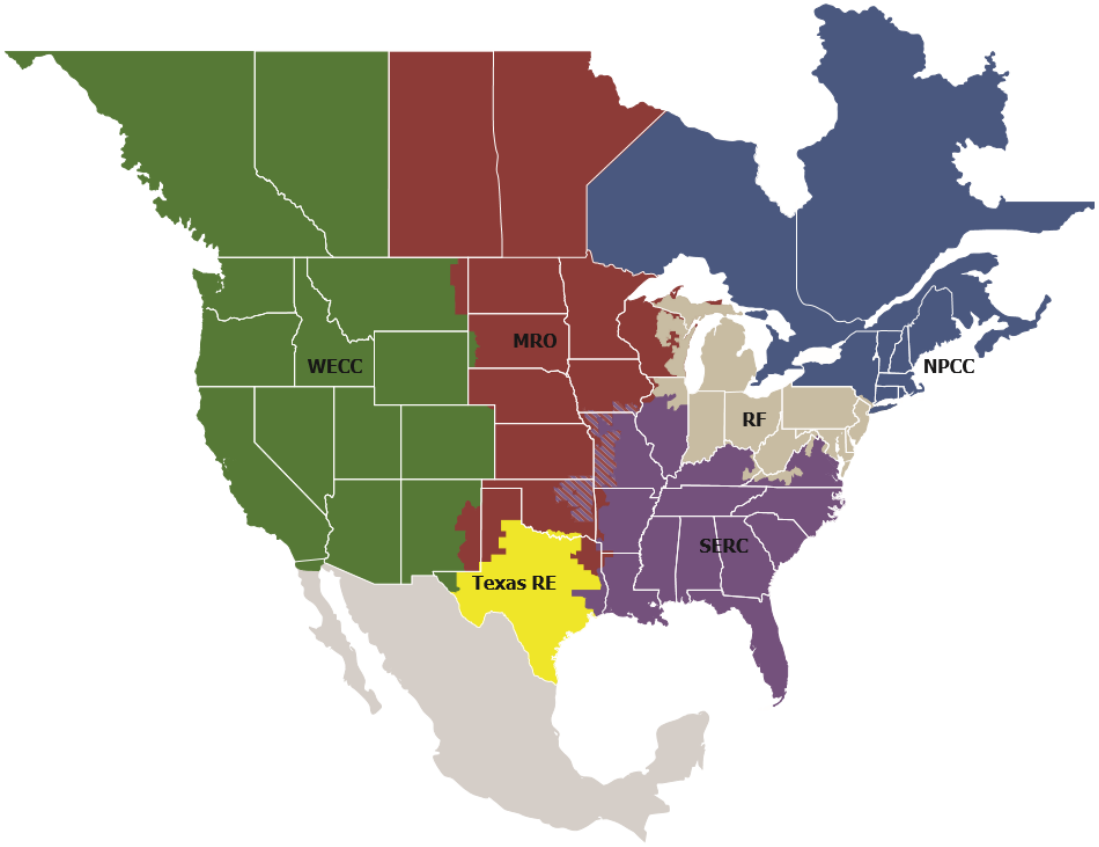
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the intent of the Standard Drafting Team (SDT) in drafting the requirements. This Technical Rationale and Justification for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving and initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT modified Reliability Standard CIP-004-X to require Responsible Entities to implement specific controls in Requirement R6 to authorize, verify, and revoke provisioned access to BES Cyber System Information (BCSI).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Requirement R1

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

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

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

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

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

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

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

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

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

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals' ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have

changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on work stations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.

Attachment 1: Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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

Requirement R2:
Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber

security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:
Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed.

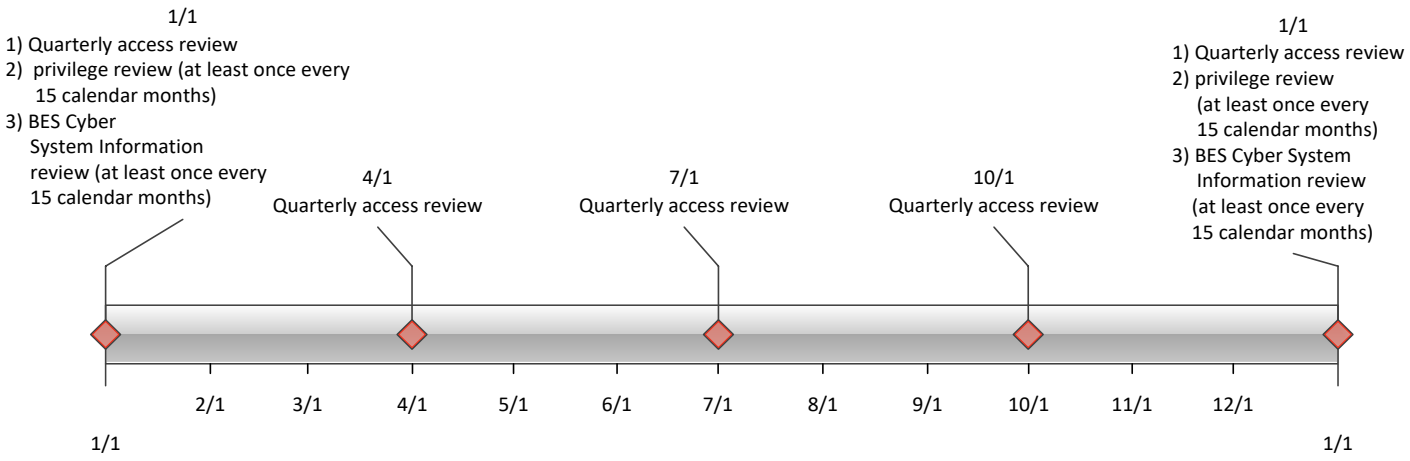
There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:
Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

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

An example timeline of all the reviews in Requirement R4 is included below.



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

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

Requirement R5:
The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts.

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

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

following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During 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:

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

Rationale for Requirement R2:

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

Rationale for Requirement R3:

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

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

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

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

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

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

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

Rationale for Requirement R5:
The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

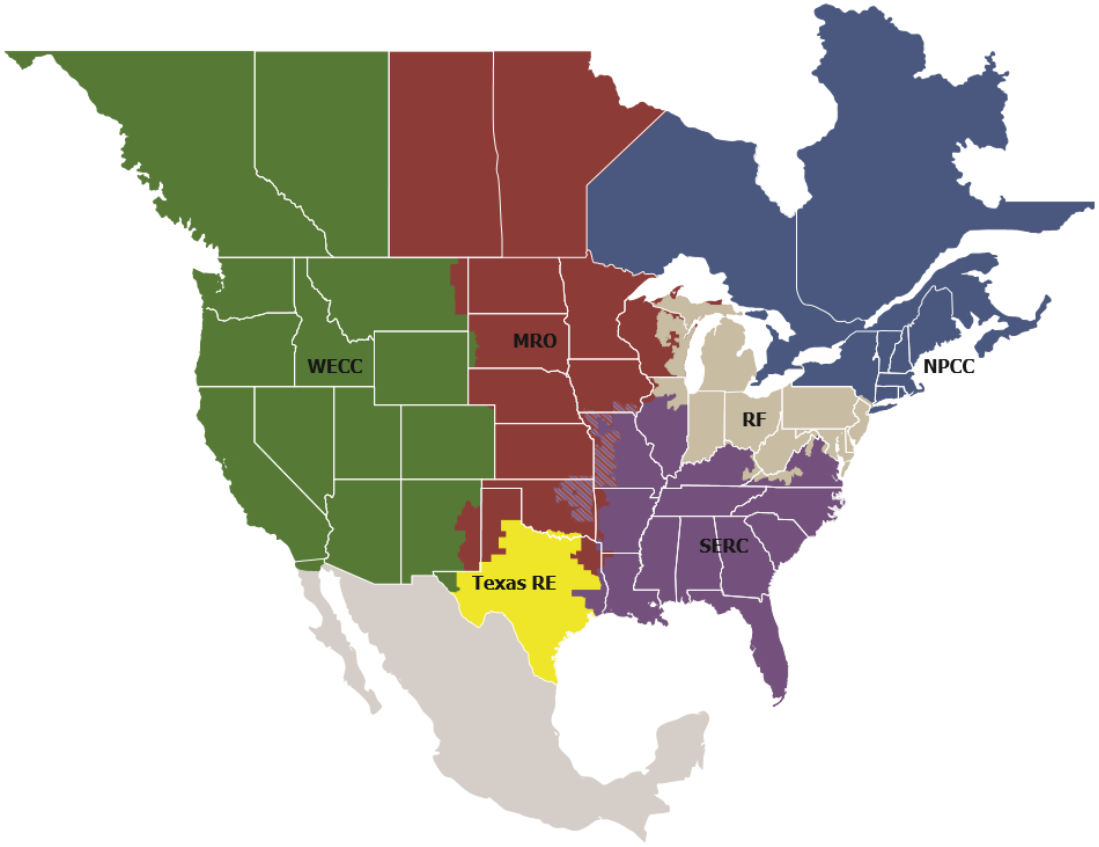
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-X. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the standard drafting team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-011-X is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 24, 2019, the North American Electric Reliability Corporation (NERC) Standards Committee accepted a Standard Authorization Request (SAR) approving an initiative to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information (BCSI), by providing a secure path towards utilization of modern third-party data storage and analysis systems. In addition, the project intended to clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

In response to this SAR, the Project 2019-02 SDT drafted Reliability Standard CIP-011-X to require Responsible Entities to implement specific methods in Requirement R1 for administrative, technical, and physical controls related to BCSI during storage, handling and use including when utilizing vendor provided cloud services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

Requirement R1

General Considerations for Requirement R1

None

Rationale for Modifications to Requirement R1:

Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1

Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Attachment 1: Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

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:

Responsible Entities are free to utilize existing change management and asset management systems.
However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information. Requirement R1 Part 1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in Requirement R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal. The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.
>
> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CDRW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

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 of Trustees approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Implementation Guidance for Reliability Standard CIP-004-X

March 2021

RELIABILITY | RESILIENCE | SECURITY




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

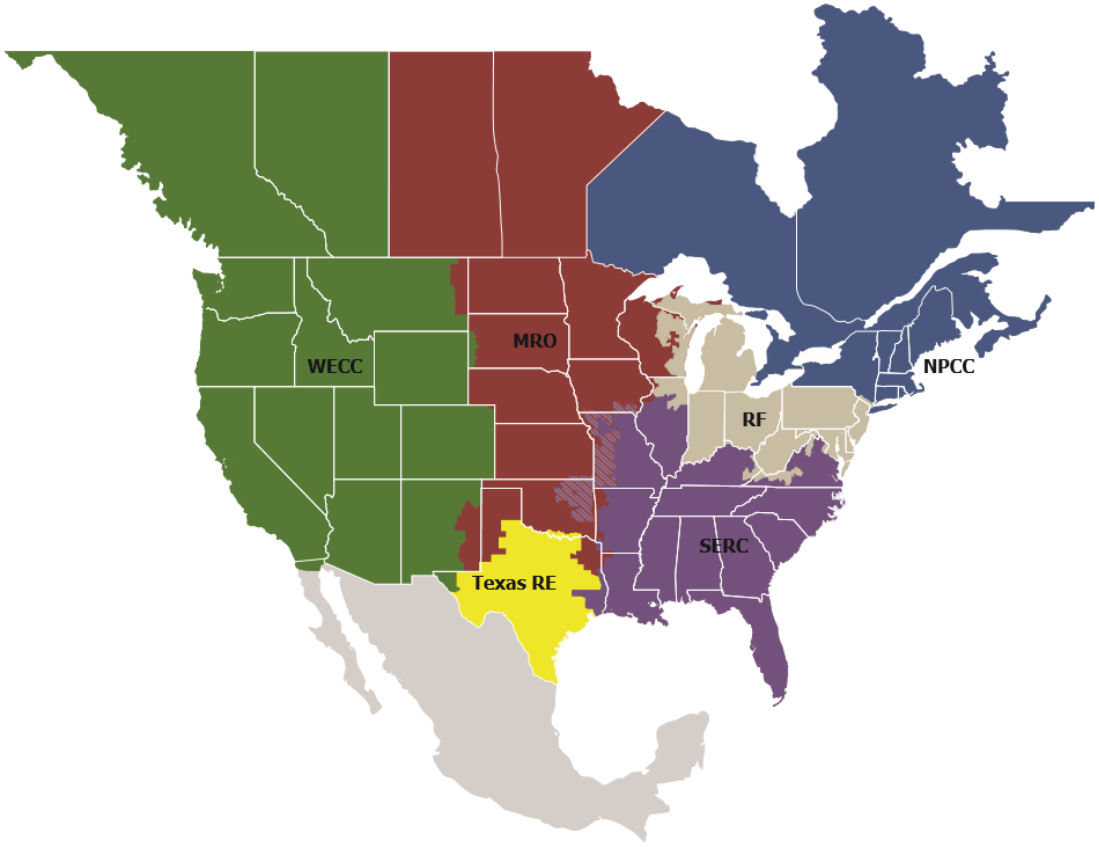
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This Implementation Guidance was prepared to provide example approaches for compliance with CIP-004-X. Implementation Guidance does not prescribe the only approach but highlights one or more approaches that could be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1] This Implementation Guidance for CIP-004-X is not a Reliability Standard and should not be considered mandatory and enforceable.

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for the modifications to CIP-004-X.

[1] NERC's Compliance Guidance Policy

Requirement R1

General Considerations for Requirement R1

None

Implementation Guidance for R1

None

Requirement R2

General Considerations for Requirement R2

None

Implementation Guidance for R2

The Responsible Entity has the flexibility to define the training program, and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles, or responsibilities at the discretion of the Responsible Entity.

Requirement R3

General Considerations for Requirement R3

None

Implementation Guidance for R3

None

Requirement R4

General Considerations for Requirement R4

None

Implementation Guidance for R4

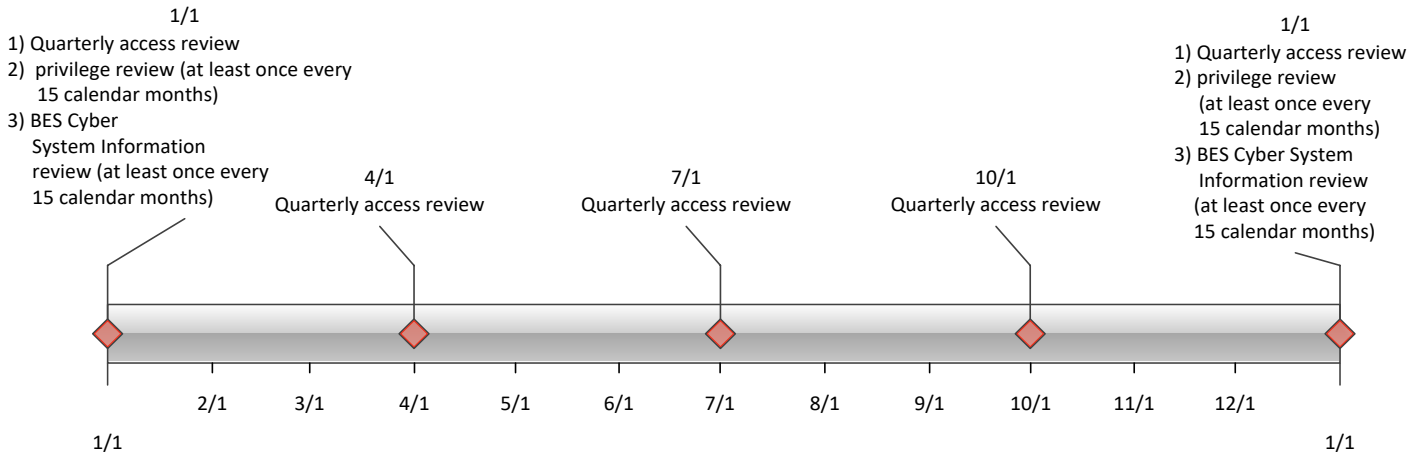
Consider including the person or persons empowered by the Responsible Entity to authorize access in the delegations referenced in CIP-003-8.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

Quarterly reviews can be achieved by comparing individuals actually provisioned access against records of individuals authorized for provisioned access. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

Entities can more efficiently perform the 15-calendar-month review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed.

An example timeline of all the reviews in Requirements R4 and R6 is included below.



Requirement R5

General Considerations for Requirement R5

None

Implementation Guidance for R5

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

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

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

If an entity considers transitioning a contracted individual to a direct hire, an entity should consider how they will meet the evidentiary requirements for Requirements R1 through R4. If evidence for compliance with Requirements R1 through R4 cannot be provided, the entity should consider invoking the applicable sub-requirements in Requirement R5 for this administrative transfer scenario. Entities should also consider including this scenario in their access management program, including a higher-level approval to minimize the instances to which this scenario would apply.

Requirement R6

General Considerations for Requirement R6

None

Implementation Guidance for R6

This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish revocation of access may include deletion or deactivation of accounts used by the individual(s). Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible. Separation of duties should also be considered when performing the 15-calendar-month verification in Requirement R6. The person reviewing should be different than the person provisioning access.

Entities may choose not to provision access, or provision temporary rather than persistent access, for authorized users. In other words, an authorized individual does not have to have any access provisioned, but all provisioned access must be authorized.

An entity can choose to give an authorization to access any BCSI, or they can have authorizations for specific storage locations or types of BCSI, if they so choose.

While Part 6.1 only requires authorization for provisioned access to BCSI, entities may also choose to have a process to authorize individuals (that is, grant them permission or make them eligible) to receive, see, or use BCSI that is disclosed to them, much like a security clearance. This can be helpful from an information protection standpoint

where individuals can be instructed to only share BCSI with others who are authorized to see it, and entities could implement this as part of their CIP-011 Information Protection Program. In this case, the review required in Requirement R6 Part 6.2 should still be performed, and the revocation required in Requirement R6 Part 6.3 could consist of removing the individual's name from the authorized list at the time of termination or upon review when it is determined the individual no longer has a need.

Entities can more efficiently perform the 15-calendar-month BCSI review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. For an example timeline to perform the 15-calendar-month BCSI review, refer to the graphic in the *Implementation Guidance for R4* section.

An example where a termination action in Requirement R5 Part 5.1, satisfies Requirement R6 Part 6.3, would be the Responsible Entity revoking an individual's means of unescorted physical access and Interactive Remote Access (e.g., physical access card, virtual private network, Active Directory user account). By revoking both physical and electronic access, the individual could ultimately not have access to BES Cyber System Information. The Responsible Entity should still revoke access that is manually provisioned (e.g., local user account, relay, site area network server, cloud based BCSI that is not tied to an active directory account).

Appendix 1: Implementation Guidance for CIP-004-6

This section contains a "cut and paste" of the Implementation Guidance components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. Similarly, former GTB content providing SDT intent and technical rationale sencan be found in a separate Technical Rational document for this standard.

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

Requirement R1:
Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:
The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Requirement R3:
Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check.

Requirement R4:
To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The list of provisioned individuals can be an automatically generated

account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

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

Requirement R5:
Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

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

Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-X. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-X, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-X, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R5
The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R5
The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-X, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-X R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

VSL Justifications for CIP-004-X R6	
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 requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby 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 VSLs are based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-X. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-X, Requirement R1

The VSL justification is below.

VSLs for CIP-011-X, R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)

VSL Justifications for CIP-011-X, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed revisions do not lower 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 VSLs are 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 VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented information protection program(s) that collectively include the applicable requirement parts in CIP-011-X Table R1 – Information Protection Program.

VRF Justification for CIP-011-X Requirement R2

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-X Requirement R2

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-004-7. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-004-7, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-7, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-7, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-7, Requirement R5
The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-7, Requirement R5
The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-7, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-7 Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified.

VRF Justifications for CIP-004-7 R6	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-7 Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-7 R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

VSL Justifications for CIP-004-7 R6	
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 requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby 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 VSLs are based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2019-02 BES Cyber System Information Access Management CIP-011-3. Each requirement is assigned a VRF and a VSL. 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 in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-011-3, Requirement R1

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3, Requirement R1

The VSL justification is below.

VSLs for CIP-011-3, R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)

VSL Justifications for CIP-011-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed revisions do not lower 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 VSLs are 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 VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to implement one or more documented information protection program(s) that collectively include the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program.

VRF Justification for CIP-011-3 Requirement R2

The VRF did not change from the previously FERC approved CIP-011-2 Reliability Standard.

VSL Justification for CIP-011-3 Requirement R2

The VSL did not change from the previously FERC approved CIP-011-2 Reliability Standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 and R5 to CIP-004-X R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	CIP-004-X, Requirement R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium]*	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes clarification on the specific elements within an access management program that need to be implemented. In addition, a definition of what constitutes BCSI access was included in the parent R6 requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	[Time Horizon: Same Day Operations and Operations Planning].	
CIP-004-6, Requirement R4, Part 4.1.3 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	**CIP-004-X, Requirement R6, Part 6.1, 6.1.1, and 6.1.2** Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	The modified requirement language includes a shift from authorizing access to designated storage locations, to authorizing the provisioned access to BCSI. The Note was included to specify the type of access to be authorized (6.1), verified (6.2) and revoked (6.3).
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	**CIP-004-X, Requirement R6, Part 6.2, 6.2.1, and 6.2.2.** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is still needed.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-6, Requirement R5, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	**CIP-004-X, Requirement R6, Part 6.3** For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.
CIP-004-6, Requirement R5, Part 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**CIP-004-6, Requirement R5, Part 5.3** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	This Part was renumbed from 5.4 to 5.3 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. The reference within the Part was changed to just Part 5.1.
CIP-004-6, Requirement R5, Part 5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the	**CIP-004-6, Requirement R5, Part 5.4** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating	This Part was renumbed from 5.5 to 5.4 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. This is a renumbering change only, no changes were made to the Part's requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Mapping of CIP-004-6 R4 and R5 to CIP-004-X R6

Access Management Program control requirements as applied to BES Cyber System Information (BCSI) designated storage locations were moved to CIP-004 Requirement R6.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	CIP-004-X, Requirement R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-X Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium]*	Requirement R6 was created to house all BCSI related access management requirements, which include the current CIP-004-6 R4.1.3, R4.4, and R5.3 in a single requirement (R6). The modified requirement language includes clarification on the specific elements within an access management program that need to be implemented. In addition, a definition of what constitutes BCSI access was included in the parent R6 requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
	[Time Horizon: Same Day Operations and Operations Planning].	
CIP-004-6, Requirement R4, Part 4.1.3 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	**CIP-004-X, Requirement R6, Part 6.1, 6.1.1, and 6.1.2** Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI. ~~Note: Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).~~	The modified requirement language includes a shift from authorizing access to designated storage locations, to authorizing the provisioned access to BCSI. The Note was included to specify the type of access to be authorized (6.1), verified (6.2) and revoked (6.3).
CIP-004-6, Requirement R4, Part 4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are	**CIP-004-X, Requirement R6, Part 6.2, 6.2.1, and 6.2.2.** Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and	The modified requirement language includes a two-part separation of the current CIP-004-6 R4.4 requirement and that the Responsible Entity 1) Verifies provisioned access to BCSI is authorized, and 2) Verifies the provisioned access is still needed.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
necessary for performing assigned work functions.	6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	
CIP-004-6, Requirement R5, Part 5.3 For termination actions, revoke the individual's current access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	**CIP-004-X, Requirement R6, Part 6.3** For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	The change in requirement language focuses on revoking the ability to use provisioned access to BCSI instead of revoking access to the designated storage locations for BCSI.
CIP-004-6, Requirement R5, Part 5.4 For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**CIP-004-6, Requirement R5, Part 5.3** For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	This Part was renumbed from 5.4 to 5.3 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. The reference within the Part was changed to just Part 5.1.
CIP-004-6, Requirement R5, Part 5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the	**CIP-004-6, Requirement R5, Part 5.4** For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the	This Part was renumbed from 5.5 to 5.4 after Part 5.3 was removed and incorporated into the new R6 Part 6.3. This is a renumbering change only, no changes were made to the Part's requirement language.

Standard: CIP-004-6		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2019-02 BES Cyber System Information Access Management

Modifications to CIP-011-X

The modifications made to requirements within CIP-011-X are intended to focus on preventing unauthorized access to BES Cyber System Information (BCSI) regardless of state (storage, transit, use).

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection Program*.	**CIP-011-X, Requirement R1.** Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to Applicable Systems that collectively includes each of the applicable requirement parts in *CIP-011-X Table R1 – Information Protection Program.*	Parent CIP-011-X Requirement R1 language modified to sharpen focus on protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems, which may contain BCSI.
CIP-011-2, Requirement R1, Part 1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.	**CIP-011-X, Requirement R1, Part 1.1** Method(s) to identify BCSI.	Requirement language simplified.

Standard: CIP-011-X		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-011-2, Requirement R1, Part 1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	**CIP-011-X, Requirement R1, Part 1.2** Method(s) to protect and securely handle BCSI to mitigate the risks of compromising confidentiality.	Requirement revised to broaden the focus around the implementation of controls that mitigate the risks of compromising confidentiality in any state, not just storage, transit, and use.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2019-02 BES Cyber System Information Access Management

Final Ballots Open through June 11, 2021

Now Available

Final ballots are open through **8 p.m. Eastern, Tuesday, June 11, 2021** for the following:

- CIP-004-X – Cyber Security - Personnel & Training
- CIP-011-X – Cyber Security - Information Protection
- Implementation Plan

Due to projects 2019-02 BES Cyber System Information Access Management (BCSI) and 2016-02 Modification to CIP Standards (2016-02) both modifying CIP-004 and CIP-011, an "-X" has been added in place of the version numbers for BCSI and a "-Y" for the 2016-02 standards. Once both projects are completed, they will be combined together with one version, prior to submission to the NERC Board.

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 pool(s) associated with this project can log into the Standards Balloting and Commenting System (SBS) and submit votes here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *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.

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

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

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: 2019-02 BES Cyber System Information Access Management CIP-004-7 FN 4 ST
Voting Start Date: 6/2/2021 12:32:01 PM
Voting End Date: 6/11/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 4
Total # Votes: 237
Total Ballot Pool: 274
Quorum: 86.5
Quorum Established Date: 6/2/2021 12:47:34 PM
Weighted Segment Value: 85.8

Actions

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	77	1	46	0.807	11	0.193	0	7	13
Segment: 2	2	0.2	1	0.1	1	0.1	0	0	0
Segment: 3	60	1	45	0.882	6	0.118	0	3	6
Segment: 4	17	1	11	1	0	0	0	2	4
Segment: 5	67	1	46	0.852	8	0.148	0	6	7
Segment: 6	44	1	25	0.735	9	0.265	0	3	7
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.6	6	0.6	0	0	0	0	0
Totals:	274	5.8	180	4.977	35	0.823	0	22	37

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Haizhen Wang		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A

5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
3	Puget Sound Energy, Inc.	Justin Rathburn		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Negative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A

1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Ryan Walter		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	Affirmative	N/A
5	Lakeland Electric	Becky Rinier	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	N/A
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	N/A
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	Negative	N/A
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Affirmative	N/A

5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason	Stefanie Burke	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane Landry		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Aidan Gallegos		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A

5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	N/A
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	N/A
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
5	Enel Green Power	Mat Bunch		Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A

5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	Affirmative	N/A
6	AEP	JT Kuehne		Negative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
3	AEP	Kent Feliks		Negative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
4	National Rural Electric Cooperative Association	Paul McCurley		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris		None	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	N/A
1	Duke Energy	Laura Lee		Negative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	N/A

5	East Kentucky Power Cooperative	David Meade	Negative	N/A
3	Wabash Valley Power Association	Susan Sosbe	Affirmative	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management CIP-011-3 FN 4 ST
Voting Start Date: 6/2/2021 12:32:45 PM
Voting End Date: 6/11/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 4
Total # Votes: 237
Total Ballot Pool: 273
Quorum: 86.81
Quorum Established Date: 6/2/2021 2:18:07 PM
Weighted Segment Value: 83

Actions

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	77	1	43	0.796	11	0.204	0	10	13
Segment: 2	2	0.2	2	0.2	0	0	0	0	0
Segment: 3	59	1	42	0.857	7	0.143	0	4	6
Segment: 4	17	1	10	1	0	0	0	3	4
Segment: 5	67	1	45	0.833	9	0.167	0	7	6
Segment: 6	44	1	24	0.727	9	0.273	0	4	7
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.6	4	0.4	2	0.2	0	0	0
Totals:	273	5.8	170	4.814	38	0.986	0	29	36

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Haizhen Wang		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Negative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A

5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
3	Puget Sound Energy, Inc.	Justin Rathburn		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Negative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Negative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
5	San Miguel Electric Cooperative, Inc.	Lana Smith		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A

5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Negative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	N/A
3	Manitoba Hydro	Mike Smith		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

3	Tri-State G and T Association, Inc.	Janelle Marriott Gill	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock	Affirmative	N/A
1	Lakeland Electric	Larry Watt	Affirmative	N/A
5	Lakeland Electric	Becky Rinier	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	N/A
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	N/A
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	Negative	N/A
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Affirmative	N/A

5	OTP - Otter Tail Power Company	Brett Jacobs		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane Landry		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Aidan Gallegos		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A

5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	N/A
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	N/A
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
5	Enel Green Power	Mat Bunch		Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A

5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	Affirmative	N/A
6	AEP	JT Kuehne		Negative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
3	AEP	Kent Feliks		Negative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
4	National Rural Electric Cooperative Association	Paul McCurley		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris		None	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	N/A
1	Duke Energy	Laura Lee		Negative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
5	East Kentucky Power Cooperative	David Meade		Negative	N/A

3	Wabash Valley Power Association	Susan Sosbe	Affirmative	N/A
5	SunPower	Bradley Collard	None	N/A
6	Evergy	Thomas ROBBEN	Affirmative	N/A
1	Evergy	Allen Klassen	Affirmative	N/A
3	Evergy	Marcus Moor	Affirmative	N/A
5	Evergy	Derek Brown	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative	N/A

Ballot Results

Ballot Name: 2019-02 BES Cyber System Information Access Management Implementation Plan FN 4 OT
Voting Start Date: 6/2/2021 12:33:47 PM
Voting End Date: 6/11/2021 8:00:00 PM
Ballot Type: OT
Ballot Activity: FN
Ballot Series: 4
Total # Votes: 231
Total Ballot Pool: 269
Quorum: 85.87
Quorum Established Date: 6/2/2021 2:18:16 PM
Weighted Segment Value: 94.17

Actions

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	76	1	48	0.923	4	0.077	0	11	13
Segment: 2	2	0.2	2	0.2	0	0	0	0	0
Segment: 3	58	1	45	0.918	4	0.082	0	4	5
Segment: 4	17	1	10	1	0	0	0	3	4
Segment: 5	65	1	46	0.92	4	0.08	0	8	7
Segment: 6	44	1	29	0.906	3	0.094	0	3	9
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.5	5	0.5	0	0	0	1	0
Totals:	269	5.7	185	5.368	15	0.332	0	31	38

Ballot Pool Members

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
5	Con Ed - Consolidated Edison Co. of New York	Haizhen Wang		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	IDACORP - Idaho Power Company	Mike Marshall		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Western Area Power Administration	sean erickson	Barry Jones	Affirmative	N/A
1	Edison International - Southern California Edison Company	Jose Avendano Mora		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A

5	Sacramento Municipal Utility District	Nicole Goi	Joe Tarantino	Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
3	Puget Sound Energy, Inc.	Justin Rathburn		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
5	Puget Sound Energy, Inc.	Lynn Murphy		Abstain	N/A
6	Western Area Power Administration	Erin Green		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
1	Puget Sound Energy, Inc.	Chelsey Neil		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A

1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat	Roger Fradenburgh	Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Platte River Power Authority	Wade Kiess		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		None	N/A
5	Florida Municipal Power Agency	Chris Gowder	Truong Le	None	N/A
4	Florida Municipal Power Agency	Dan O'Hagan	Truong Le	None	N/A
3	Florida Municipal Power Agency	Carl Turner	Truong Le	None	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Truong Le	None	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Abstain	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
3	Lakeland Electric	Steve Marshall		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		None	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		None	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
1	Lakeland Electric	Larry Watt		Affirmative	N/A

5	Lakeland Electric	Becky Rinier	Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	Affirmative	N/A
3	Eversource Energy	Christopher McKinnon	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston	Abstain	N/A
5	Oglethorpe Power Corporation	Donna Johnson	Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz	None	N/A
1	Black Hills Corporation	Seth Nelson	None	N/A
5	Black Hills Corporation	Derek Silbaugh	Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith	Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien	Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci	Negative	N/A
6	New York Power Authority	Erick Barrios	Affirmative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt	None	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price	Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder	Negative	N/A
3	Muscatine Power and Water	Seth Shoemaker	Abstain	N/A
6	Muscatine Power and Water	Nick Burns	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	N/A
3	Westar Energy	Bryan Taggart	None	N/A
6	Westar Energy	Grant Wilkerson	None	N/A
5	Southern Company - Southern Company Generation	James Howell	Affirmative	N/A
6	Manitoba Hydro	Simon Tanapat-Andre	None	N/A
5	Tennessee Valley Authority	M Lee Thomas	Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Joseph Neglia	Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman	Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl	Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund	None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey	Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons	Abstain	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	Abstain	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden	Affirmative	N/A
5	OTP - Otter Tail Power Company	Brett Jacobs	None	N/A

3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
5	JEA	John Babik		None	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	David Reinecke		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane Landry		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Aidan Gallegos		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

1	Santee Cooper	Chris Wagner		Affirmative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle Longo		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Truong Le	None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	Great River Energy	Donna Stephenson		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Powerex Corporation	Raj Hundal		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
5	Exelon	Cynthia Lee		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
5	Enel Green Power	Mat Bunch		Abstain	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
		Kammy Rogers-			

1	Bonneville Power Administration	Holliday		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Great River Energy	Jacalynn Bentz		Negative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Byron Booker	Abstain	N/A
6	AEP	JT Kuehne		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
3	AEP	Kent Feliks		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
4	National Rural Electric Cooperative Association	Paul McCurley		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
1	Arkansas Electric Cooperative Corporation	Jennifer Loiacano		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
5	Arkansas Electric Cooperative Corporation	Adrian Harris		None	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
5	East Kentucky Power Cooperative	David Meade		Negative	N/A
3	Wabash Valley Power Association	Susan Sosbe		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

3	Evergy	Marcus Moor	Affirmative N/A
5	Evergy	Derek Brown	Affirmative N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy	Affirmative N/A
6	FirstEnergy - FirstEnergy Corporation	Ann Carey	Affirmative N/A

Exhibit I

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2019-02 BES Cyber System Information Access Management

	Name	Entity
Chair	John Hansen	Exelon
Vice Chair	Josh Powers	Southwest Power Pool, Inc. (SPP)
Members	Victoria Bethley	Duke Energy
	Andrew Camargo	San Diego Gas & Electric
	Sharon Koller	American Transmission Company, LLC
	Michael Lewis	Southern California Edison
	Conor Martin	Arizona Public Service
	Yoel Piney	PSEG
	Regan Plain	Minnkota Power Cooperative
	Joshua Roper	Westar and KCP&L, Evergy Companies
	Clay Walker	Cleco Corporate Holdings LLC
	William Vesely	Consolidated Edison Company of New York, Inc.
PMOS Liaison(s)	Colby Bellville	Cooperative Energy
	Kirk Rosener	CPS Energy
NERC Staff	Latrice Harkness – Senior Standards Developer	North American Electric Reliability Corporation
	Marisa Hecht – Legal	North American Electric Reliability Corporation
	Lauren Perotti – Legal	North American Electric Reliability Corporation