UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-015-1

Lauren A. Perotti
Assistant General Counsel
Sarah P. Crawford
Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Counsel for the North American Electric Reliability Corporation

June 24, 2024

TABLE OF CONTENTS

Exhibit A	The Proposed Reliability Standard
Exhibit B	Implementation Plan
Exhibit C	Technical Rationale
Exhibit D	Order No. 672 Criteria
Exhibit E	Analysis of Violation Risk Factors and Violation Severity Levels
Exhibit F	Summary of Development and Complete Record of Development
Exhibit G	Standard Drafting Team Roster, Project 2023-03 Internal Network Security Monitoring (INSM)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-015-1

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5[2] of the Federal Energy Regulatory Commission's ("FERC" or "Commission") regulations, and the Commission's January 19, 2023 order in Docket No. RM22-3-000,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval proposed Reliability Standard CIP-015-1 (Cyber Security - Internal Network Security Monitoring).[5]

Proposed Reliability Standard CIP-015-1 would advance reliability by establishing requirements for internal network security monitoring for network traffic inside an Electronic Security Perimeter ("ESP"). Such monitoring would improve the probability of detecting anomalous or unauthorized network activity, thus facilitating an improved response to and recovery from an attack. The proposed Reliability Standard addresses FERC's directives in Order

---

1 16 U.S.C. § 824o.

2 18 C.F.R. § 39.5 (2023).

3 *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023) [hereinafter Order No. 887].

4 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006), *order on reh'g & compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

5 Unless otherwise indicated, all capitalized terms used in this petition shall have the meaning set forth in the *Glossary of Terms used in NERC Reliability Standards* ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

No. 887 that NERC modify the Critical Infrastructure Protection ("CIP") Reliability Standards to provide such protections.

NERC requests that the Commission approve the proposed Reliability Standard CIP-015-1, as shown in **Exhibit A**, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also requests that the Commission approve: (i) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (**Exhibit E**); and (ii) the proposed implementation plan (**Exhibit B**).

As required by Section 39.5(a)[6] of the Commission's regulations, this petition presents the technical basis and purpose of the proposed Reliability Standard, a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672[7] (**Exhibit D**), and a summary of the standard development history (**Exhibit F**). The NERC Board of Trustees adopted the proposed Reliability Standard on May 9, 2024.

This petition is organized as follows: Section I provides a summary of the proposed Reliability Standard and Order No. 887, which led to its development. Section II of the petition provides the individuals to whom notices and communications related to the filing should be provided. Section III provides relevant background regarding the regulatory structure governing the Reliability Standards approval process. Section IV provides a brief summary of the development process for the proposed Reliability Standard. Section V of the petition addresses the need for internal network security monitoring. Section VI of the petition provides an overview and

---

[6] 18 C.F.R. § 39.5(a).

[7] The Commission specified in Order No. 672 certain general factors it would consider when assessing whether a particular Reliability Standard is just and reasonable. *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 P 262, 321-37 ("Order No. 672"), *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

justification for the proposed Reliability Standard. Section VII of the petition provides a summary of the proposed implementation plan.

I. SUMMARY

The CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the Bulk Electric System ("BES") against cyber and physical security threats. This approach requires BES Cyber Systems or Facilities that could have the highest impact to the grid receive the highest level of protections. In other words, the level of controls required for protecting cyber systems is in proportion to the risk each system presents to reliable operation of the Bulk-Power System ("BPS"). This approach is used to help ensure resources are appropriately allocated to mitigate the risk of malicious actors targeting specific assets or electric power entities because of their potential impact to the grid.

On January 19, 2023, FERC issued Order No. 887 that directed NERC to develop new or modified CIP Reliability Standards that require internal network security monitoring for CIP-networked environments for all high impact bulk electric system BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.[8] In response to Order No. 887, NERC initiated Project No. 2023-03, Internal Network Security Monitoring. The Project 2023-03 drafting team developed new Reliability Standard CIP-015-1, which establishes requirements for internal network security monitoring for network traffic inside an Electronic Security Perimeter. The proposed Reliability Standard would improve the probability of detecting anomalous or unauthorized network activity and facilitate an improved response to and recovery from an attack.

[8] Order No. 887 at P 1.

Proposed Reliability Standard CIP-015-1 would require Responsible Entities to implement internal network security monitoring systems and processes. Specifically, Responsible Entities would evaluate their networks within Electronic Security Perimeters and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities would then be required to collect, analyze, and respond appropriately to anomalous activity within applicable networks. Responsible Entities would also be required to evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. In addition, the proposed standard would require Responsible Entities to protect relevant network data collected under the standard to prevent unauthorized data manipulation, and to preserve the data, as needed, for additional investigation.[9]

Proposed Reliability Standard CIP-015-1 would advance the reliability of the BPS by providing a comprehensive suite of requirements for internal network security monitoring, that are forward looking and objective-based, consistent with Order No. 887. NERC respectfully requests that the Commission approve proposed Reliability Standard CIP-015-1 and the associated elements 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

[9] Exhibit C Technical Rationale at 2.

following:[10]

Lauren A. Perotti*
Assistant General Counsel
Sarah P. Crawford*
Counsel
North American Electric Reliability Corporation
1401 H Street NW
Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Soo Jin Kim*
Vice President, Engineering and Standards
Alison Oswald *
Manager, Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile
soo.jin.kim@nerc.net
alison.oswald@nerc.net

III. REGULATORY BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[11] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the BPS, and with the duties of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1)[12] of the FPA states that all users, owners, and operators of the BPS in the United States will be subject to Commission-approved Reliability Standards. Section 215(d)(5)[13] of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Section 39.5(a)[14] of the Commission's regulations requires the ERO to file with the Commission for its approval each new Reliability

[10] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[11] 16 U.S.C. § 824o.

[12] *Id.* § 824o(b)(1).

[13] *Id.* § 824o(d)(5).

[14] 18 C.F.R. § 39.5(a).

Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes should be made effective.

The Commission is vested with the regulatory responsibility to approve Reliability Standards that protect the reliability of the BPS and to ensure that Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA[15] and Section 39.5(c)[16] of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process. NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[17]

In its order certifying NERC as the Commission's ERO, the Commission found that NERC's rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards,[18] and thus satisfy several of the Commission's criteria for approving Reliability Standards.[19] The development process is open to any person or entity with a legitimate interest in the reliability of the BPS. NERC considers the comments of all stakeholders. Stakeholders must approve, and the NERC Board of Trustees

---

15 16 U.S.C. § 824o(d)(2).

16 18 C.F.R. § 39.5(c)(1).

17 The NERC Rules of Procedure, including Appendix 3A, NERC Standard Processes Manual, are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

18 *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, at P 250 (2006).

19 Order No. 672 at PP 268, 270.

must adopt, a new or revised Reliability Standard before NERC submits the Reliability Standard to the Commission for approval.

IV. SUMMARY OF DEVELOPMENT, PROJECT 2023-03 INTERNAL NETWORK SECURITY MONITORING

On January 19, 2023, FERC issued Order No. 887. In this order, FERC directed NERC to develop new or modified CIP Reliability Standards that require internal network security monitoring for CIP-networked environments for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.[20] The Commission also directed NERC to submit a report within 12 months of the issuance of Order No. 887 that studied the feasibility of implementing internal network security monitoring at all low impact BES Cyber Systems and medium impact Cyber Systems without external routable connectivity.[21]

In response to Order No. 887, NERC initiated Project No. 2023-03, Internal Network Security Monitoring. NERC also submitted the Internal Network Security Monitoring Feasibility Study Report in Docket No. RM22-3-00 on January 18, 2024.

For the initial posting, the drafting team proposed modifications to CIP-007. The initial posting ran from December 14, 2023 – January 17, 2024. [22] The initial ballot failed to achieve the required ballot body approval.

---

20 Order No. 887 at P 1.

21 *Id.*

22 On August 8, 2023, the Standards Committee approved a waiver under Section 16.0 of the Standard Processes Manual to allow shorter than usual periods for comment and ballot for this project. Specifically, the Standards Committee approved shortening the initial formal comment and ballot period from 45 days to as few as 30 calendar days, with ballot pools formed in the first 20 days, and shortening the additional formal comment and ballot period(s) from 45 days to as few as 20 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period; and shortening the final ballot from 10 days to as few as five calendar days.

In reviewing the stakeholder feedback from the initial posting, the drafting team determined that revising Reliability Standard CIP-007 did not fully align with the drafting team's objectives. Specifically, the drafting team noted that Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access Control or Monitoring Systems ("EACMS"), Physical Access Control Systems ("PACS"), and Protected Cyber Assets ("PCA"), which does not align perfectly with the scope of internal network security monitoring, which is more focused on the data communicated within the networks containing BES Cyber Systems.[23]

Based on the feedback received during the initial posting, the drafting team decided to create a new Reliability Standard, designated as Reliability Standard CIP-015-1. The drafting team concluded that this approach would better align with the directives set forth by Order No. 887 by exclusively focusing on the establishment of internal network security monitoring for network traffic inside an Electronic Security Perimeter to improve the probability of detecting anomalous or unauthorized network activity and to facilitate an improved response to and recovery from an attack. Creating a new standard also ensures maximum flexibility for future modifications, if needed.[24]

---

23 Exhibit C Technical Rationale at 3.

24 *Id.*

The first draft of proposed Reliability Standard CIP-015-1 was posted for an additional formal comment period and ballot from February 27, 2024 – March 18, 2024.[25] The additional ballot failed to achieve the required ballot body approval.[26]

A revised draft of Reliability Standard CIP-015-1 was posted for an additional formal comment period and ballot from April 5, 2024 – April 17, 2024, where it achieved the required ballot body approval. The proposed Reliability Standard was posted for a final ballot from April 24, 2024 – April 30, 2024 and achieved the following approval percentages:

- Proposed Reliability Standard CIP-015-1: 76.56% approval / 93.36% quorum; and
- Implementation Plan: 82.1% approval / 91.31% quorum.

The NERC Board of Trustees adopted the proposed Reliability Standard on May 9, 2024. A summary of the development history and the complete record of development is attached to this petition as **Exhibit F**.

V. THE NEED FOR INTERNAL NETWORK SECURITY MONITORING

The risk-based construct of the CIP Reliability Standards requires users, owners, and operators of the BES to identify their cyber systems (referred to as BES Cyber Systems) that could have an adverse effect on BES reliability if lost, compromised, or misused. Using bright-line criteria, responsible entities must then categorize their BES Cyber Systems as high, medium, or low impact based on the risks they present to the grid if lost, compromised, or misused. Once these BES Cyber Systems are identified and categorized, the CIP Reliability Standards require

[25] This posting was the first posting of Reliability Standard CIP-015-1; however, it was treated as additional formal comment and ballot period for Project 2023-03 under NERC's *Standard Processes Manual* because the Project 2023-03 drafting team had posted revisions to CIP-007 in the initial posting in response to the directives from Order No. 887. The drafting team subsequently decided to create a new CIP-015-1 standard rather than continuing to pursue revisions to CIP-007.

[26] On February 21, 2024, the Standards Committee granted the drafting team's second request for a waiver to further shorten additional formal comment and ballot periods from 45 days to as few as 10 calendar days with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period.

responsible entities to, among other things, establish plans, protocols, and controls to protect those systems against a cyber or physical attack, train personnel on security matters, report security incidents, and recover from security events.

In Order No. 887, the Commission found that "while the CIP Reliability Standards require monitoring of the electronic security perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This presents a gap in the currently effective CIP Reliability Standards."[27] To address this gap, FERC directed NERC to "develop new or modified CIP Reliability Standards requiring [internal network security monitoring] for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress."[28]

FERC explained that "[internal network security monitoring] is a subset of network security monitoring that is applied within a 'trust zone,'[29] such as an electronic security perimeter",[30] and that for the purpose of Order No. 887, "the trust zone applicable to [internal network security monitoring] is the CIP-networked environment."[31] FERC further explained that

---

27 Order No. 887 at P 3.

28 *Id.*

29 *Id.* at P 2 & n.6 (referencing The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) defines trust zone as a "discrete computing environment designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone." CISA, *Trusted Internet Connections 3.0: Reference Architecture*, at 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf.).

30 Order No. 887 at P 2.

31 *Id.*

internal network security monitoring consists of three stages: (1) collection; (2) detection; and (3) analysis.[32] Specifically, FERC directed NERC to develop requirements for any new or modified CIP Reliability Standards that are "forward-looking, objective-based"[33] and address the following three security objectives:

> (1) the need for Responsible Entities to develop baselines of their network traffic inside their CIP-networked environment;
>
> (2) the need for Responsible Entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and
>
> (3) the need to require Responsible Entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.[34]

Order No. 887 provided that internal network security monitoring will "enabl[e] continuing visibility over communications between networked devices within a trust zone and detection of malicious activity that has circumvented perimeter controls",[35] and "facilitate[e] the detection of anomalous network activity indicative of an attack in progress, thus increasing the probability of early detection and allowing for quicker mitigation and recovery from an attack."[36] FERC directed NERC to submit these revisions within 15 months of the final rule's effective date.[37]

---

32 *Id.* at P 9 (citing Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2020/applied-collection-framework).

33 *Id.* at P 5.

34 *Id.*

35 *Id.* at P 2.

36 *Id.*

37 *Id.* at P 6.

VI. JUSTIFICATION FOR APPROVAL

In this petition, NERC submits for Commission approval proposed Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring. As discussed below and in **Exhibit C**, the proposed Reliability Standard would address the Commission's directives in Order No. 887 by establishing three requirements for Responsible Entities to implement internal network security monitoring systems and processes. Under Requirement R1, Responsible Entities would be required to collect and monitor electronic communications within Electronic Security Perimeter environments.[38] Responsible Entities would further be required to analyze the detected anomalous activity and take appropriate action. Requirement R2 would require Responsible Entities to establish a process for retaining internal network security monitoring data associated with anomalous network activity. Requirement R3 would require Responsible Entities to appropriately protect the collected internal network security monitoring related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation.[39]

As discussed in **Exhibit D**, the proposed Reliability Standard meets the Commission's criteria for approval in Order No. 672 and is just, reasonable, not unduly discriminatory, and in the public interest. NERC respectfully requests that the Commission approve the proposed Reliability Standard, to become effective in accordance with the proposed implementation plan discussed in Section VII.

A. Proposed Reliability Standard CIP-015-1 Advances the Reliability of the Bulk-Power System Through Targeted Requirements Focused on Network Data Flows within the Electronic Security Perimeter

[38] Exhibit C Technical Rationale at 4.

[39] *Id.* at 17.

As a foundational matter, proposed Reliability Standard CIP-015-1 applies to network data feeds within the Electronic Security Perimeter. This complies with the Commission's directives to develop a standard requiring internal network security monitoring for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress.[40] It further takes into account the language in Order No. 887 that internal network security monitoring should be applied within a trust zone,[41] "such as the electronic security perimeter",[42] and that for the purpose of Order No. 887, "the trust zone applicable to [internal network security monitoring] is the CIP-networked environment."[43]

The appropriate scope for the proposed internal network security monitoring requirements was the subject of much debate in the underlying standard development proceeding. Early in Project 2023-03, the drafting team considered several alternatives as to what network data flows may be included within internal network security monitoring. For example, in the initial posting, the drafting team proposed a broader scope for the proposed requirements than in the final version. Specifically, the drafting team proposed including network data from EACMS and PACS outside the Electronic Security Perimeter. Drawing on its technical expertise, as well as a fulsome consideration of the comments received throughout the standard development process, the drafting team narrowed the focus of proposed Reliability Standard CIP-015-1 to include the network data

---

40 Order No. 887 at P 3.

41 *Id.* at P 2 & n.6 (The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) defines trust zone as a "discrete computing environment
designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone." CISA, *Trusted Internet Connections 3.0: Reference Architecture*, at 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf).

42 *Id.* at P 2 & n.7 ("An electronic security perimeter is 'the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol'." NERC Glossary).

43 *Id.* at P 2.

flows within the Electronic Security Perimeter. This determination reflects the fact that Reliability Standard CIP-002 requires the categorization of BES Cyber Systems and associated BES Cyber Assets that if rendered unavailable, degraded, or misused could, within 15 minutes adversely impact the reliable operation of the BES. Moreover, Reliability Standard CIP-005 requires that all applicable Cyber Assets connected to a network via routable protocol shall reside within a defined Electronic Security Perimeter.[44] Thus, the devices supporting the reliable operation of the BES are contained within an Electronic Security Perimeter. As a result, the drafting team determined that its approach for proposed Reliability Standard CIP-015-1 would comply with the directives set forth in Order No. 887 and provide the greatest benefit to the reliability of the Bulk-Power System by focusing limited industry resources on the most critical environments, i.e., those network data flows within the Electronic Security Perimeter, while advancing the risk-based focus of the CIP Reliability Standards.

This determination was supported by multiple comments stating that expanding the scope beyond the most critical environments for monitoring (i.e., beyond the Electronic Security Perimeter) could have the unintended effect of impeding an entity's ability to detect and respond to threats to their most critical systems. For example, one commenter stated:

> [m]oving beyond the [BES Cyber Systems] and outside the [Electronic Security Perimeter] takes the focus off the most critical environments for monitoring. [Internal network security monitoring] systems are likely to generate extreme volumes of data as entities mature their implementations. Large data volumes will require significant investment of time and resources to generate meaningful baselines of network traffic, especially for large entities with diverse software solutions across their various [BES Cyber Systems] and EACMS. An unclear and overly large scope for the initial [internal network security monitoring] implementation threatens to create alarm/alert fatigue that will hamper the ability of

[44] *See* Exhibit C Technical Rationale at 3.

> entities to detect and respond to threats to their most critical systems residing within their [Electronic Security Perimeters].[45]

Other comments noted the need for a risk-based focus, stating, "[t]he standard should be focused on BES Cyber Systems and PCAs (e.g., those systems inside the [Electronic Security Perimeter]). Inclusion of non-BES Cyber Assets, coupled with the ambiguity of non-glossary defined criterion is overly broad and diminishes the focus on protecting the most important systems."[46]

In addition, the drafting team considered other comments stating that the inclusion of EACMS and PACS outside the Electronic Security Perimeter would not provide a reliability benefit commensurate with the cost and complexity of implementation.[47] One commenter stated, "[i]ncluding EACMS and PACS in the scope, significantly increases the cost and complexity of the [internal network security monitoring] requirement as many PACS are spread throughout different geographical locations and networks, significantly increasing the cost and complexity of implementing the requirements, with little security benefit to gain since any attack would likely come from a Cyber Asset that is not classified as an EACMS or PACS."[48] Similarly, a different

---

45 NERC, *Consideration of Comments* – Project 2023-03 Internal Network Security Monitoring, February 2024 (Exhibit F Summary of Development and Complete Record of Development, item 19) at 62 (Duke Energy (Duke)).

46 NERC, *Consideration of Comments* - Project 2023-03 Internal Network Security Monitoring, February 2024 (Exhibit F Summary of Development and Complete Record of Development, item 19) at 21 (Tennessee Valley Authority (TVA)); *see also* Comments of Sacramento Municipal Utility District (Sacramento Municipal Utility District (SMUD): "[i]ncluding EACMS and PACS in the requirement for INSM, where monitoring is only required between them, does not further the reliability and security inside the CIP networked environment.") at 63.

47 *See Id.* at 419-420, Comments of Southwest Power Pool: ((("SPP asks the [drafting team] to consider the potential cost that may arise from the scope of this requirement. As noted in other supporting documents related to [internal network security monitoring], the costs associated with capturing, analyzing, and storing of all data between every cyber assets [sic] within an [Electronic Security Perimeter], for any length of time, will be substantial. Not all network architectures are created equal and could be more costly and time consuming to implement for some Responsible Entities than others. Virtualization of network, server, and storage infrastructure, and the complexity it brings to the table, has the potentiality to make packet captures, baselining of traffic, monitoring, analyzing, and alerting much more difficult if a Responsible Entity is unable to obtain visibility into all of the network traffic within a subnet.").

48 *Id.* at 104-105, (SMUD); *see also* Comments of Calpine Corporation: ("A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS.") at 114.

commenter asserted that "[t]he reliability gained by requiring [internal network security monitoring] on this subset of systems does not outweigh the increased cost or additional documentation needed to prove compliance."[49] A third commenter stated that "[a]ddressing boundary-level (north-south) controls for these assets would be more cost-effective approach and a logical first step to creating a common understanding of a "trust zone" for these device types before an east-west monitoring construct is applied."[50]

Finally, the drafting team determined that the scope of proposed Reliability Standard CIP-015-1 was consistent with the plain language of Order No. 887. As noted above, Order No. 887 provided that internal network security monitoring should apply within a trust zone,[51] "such as the electronic security perimeter".[52] Order No. 887 further provided that "the trust zone applicable to [internal network security monitoring] is the CIP-networked environment."[53] When determining the scope for the proposed standard under Order No. 887, the drafting team considered that CIP-networked environment is not defined within Order No. 887, nor is it defined in the NERC Glossary of Terms.[54] The drafting team looked to the plain language of Order No. 887 that stated that internal network security monitoring should apply within a trust zone,[55] "such as the electronic security perimeter"[56] and took into account that Order No. 887 did not mention including EACMS and PACS outside of the Electronic Security Perimeter.[57] Some commenters suggested that the

49 *Id.* at 106 (Eversource Energy).

50 *Id.* at 423 (Duke).

51 Order No. 887 at P 2 & n.6 (internal citations omitted).

52 *Id.* at P 2.

53 *Id.*

54 Exhibit C Technical Rationale at 3.

55 Order No. 887 at P 2 & n.6 (internal citations omitted).

56 *Id.* at P 2.

57 Exhibit C Technical Rationale at 3.

exclusion of EACMS and PACS from Order No. 887 may have been intentional;[58] other commenters observed that including EACMS and PACS outside an Electronic Security Perimeter or "trust zone,"[59] would result in applying internal network security monitoring to *external* communications, rather than *internal.*[60] Based on a fulsome consideration of Order No. 887 and the standard development record, the drafting team focused proposed Reliability Standard CIP-015-1 on the most critical "trust zone", the networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity.

B. Purpose and Applicability

The purpose of proposed Reliability Standard CIP-015-001 is "[t]o improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack." Proposed Reliability Standard CIP-015-001 would advance the

---

58 NERC, *Consideration of Comments* – Project 2023-03 Internal Network Security Monitoring, February 2024 (Exhibit F Summary of Development and Complete Record of Development, item 19) at 109 (Network and Security Technologies); ("[t]here is no mention in the Order of 'CIP' devices that may be outside [Electronic Security Perimeters], such as EACMS and PACS, and we believe this was in fact intentional."); *see also* Comments of Georgia System Operations Corporation ("The FERC order specifically addressed High and Medium-Impact assets. Extending the proposed standard to associated EACMS and PACS exceeds the scope of the FERC order and they should be removed.") at 128; Comments of Avista Corporation ("[w]e believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the 'CIP-Network Environment' then it should be out of scope as well.") at 121; Comments of Duke Energy ("[w]e do not support the interpretation that the CIP-networked environment is inclusive of EACMS and PACS-classified cyber assets that do not reside within an ESP.") at 61-62.

59 *Id.* at 104 (SMUD) ("[i]ncluding EACMS and PACS, which are not required to be protected by an ESP, Electronic Access Point (EAP), or required to be in a 'trust zone' does not align with intent of the SAR or the FERC Order, which is to perform network monitoring of traffic between devices *within* a trusted zone."); Comments of North American Generator Forum (NAGF): (NAGF "would refer the [drafting team] back to Order [No.] 887 in that the network traffic in scope for INSM is communications within an ESP between other Cyber Assets within that "trust zone" also referred to as east west traffic. The inclusion of EACMS and PACS goes beyond the scope of INSM and the current Draft 1 creates confusion as to the intent of the requirements commingling 'Network Security Monitoring' principles which include devices outside of the [Electronic Security Perimeter] or 'trust zones.") at 115-116.

60 *Id.* at 99 (Pacific Gas and Electric Company (PG&E)) ("[t]he FERC Order was for 'internal' communications, but the current language does not clearly indicate this and could be interpreted by auditors to include traffic outside of the ESP, such as those to PACS and EACMS outside of the ESP. PG&E recommends to clearly indicate that communications outside of the ESP to devices such as PACS and EACMS are not in scope.").

reliability of the BPS by establishing three requirements that would require Responsible Entities to evaluate their networks within Electronic Security Perimeters and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations; collect, analyze, and respond appropriately to anomalous network communications within applicable networks; and protect the collected internal network security monitoring related network communications data to prevent unauthorized data manipulation and preserve the data to facilitate additional investigation.[61]

The applicability for proposed Reliability Standard CIP-015-1 would include the following: Balancing Authorities, Distribution Providers, Generator Owners, Generator Operators, Reliability Coordinators, Transmission Owners, and Transmission Operators.

C. Requirement R1

Proposed Reliability Standard CIP-015-1, Requirement R1 consists of a requirement with three Parts that would establish a process for detecting and evaluating anomalous network activity by establishing internal network security monitoring of networks protected by an Electronic Security Perimeter(s) for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. Proposed Requirement R1 would addresses the directives in Order No. 887 that Responsible Entities (1) develop baselines of their network traffic inside their CIP-networked environment; (2) monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) identify anomalous activity.[62]

---

61 Exhibit C Technical Rationale at 2.

62 Order No. 887 at P 5.

Proposed Requirement R1 would require Responsible Entities to collect and monitor network communications within Electronic Security Perimeter environments. Proposed Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities would create a documented process for collecting and analyzing network traffic. As used in proposed Requirement R1 and Requirement R1, Part 1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic.[63] The proposed Requirement R1 and Parts 1.1, 1.2, and 1.3 are shown below:

> **R1.** Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts:
>
> **1.1.** Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
>
> **1.2.** Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
>
> **1.3.** Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

1. Requirement R1, Part 1.1

Proposed Requirement R1, Part 1.1 would require that the Responsible Entity "[i]mplement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications." Specifically, the Responsible Entity, using a risk-based rationale, would identify possible network data collection locations and then may narrow the actual collected data to the data feeds that contain the most cost-effective and

[63] Exhibit C Technical Rationale at 12.

relevant data for cyber security monitoring purposes.[64] A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds such as: a risk analysis, an impact analysis, or an analysis of common adversarial techniques.[65] Allowing a risk-based rationale would afford Responsible Entities the opportunity to make informed decisions based on their unique network architecture, which may be vastly different from that of other Responsible Entities. This would promote innovative outcomes to meet reliability objectives, rather than prescribing a one size-fits all approach that may not be the most effective solution for the variety of network topologies. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.[66]

Under proposed Requirement R1, Part 1.1, Responsible Entities would evaluate their Electronic Security Perimeter networks and select and implement one or more internal network security monitoring network data feed(s)[67] in each Electronic Security Perimeter. These data feeds would provide the necessary data to implement proposed Requirement R1, Parts 1.2. and 1.3. Thus, proposed Requirement R1, Part 1.1. would allow Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.[68]

---

64 Exhibit C Technical Rationale at 5.

65 *Id.*

66 *Id.*

67 A network data feed is the combination of a data collection location and a data collection method. Collection methods are technologies that provide visibility of network data to an INSM system (examples are provided below). In context of Reliability Standard CIP-015-1, network locations are physical or virtual devices that move data on a network. These devices include switches, virtual switches, firewalls, routers, network interfaces and similar devices. *See* Exhibit C Technical Rationale at 5.

68 Exhibit C Technical Rationale at 5.

2. Requirement R1, Part 1.2

Proposed Requirement R1, Part 1.2 would require a Responsible Entity to "[i]mplement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1." Detecting anomalous network activity would include processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.[69] Anomalous traffic by itself would not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in proposed Requirement R1, Part 1.3. The Responsible Entity should implement detection methods[70] that, as part of an overall internal network security monitoring program, would provide data necessary for analysts to identify anomalous activity to a high level of confidence.[71]

3. Requirement R1, Part 1.3

Proposed Requirement R1, Part 1.3 would require Responsible Entities to "implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)." Evaluation of detected anomalous activity would be implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their internal network security monitoring process(es) developed in Requirement R1.[72] The aim of the requirement is to arm the entity with the information needed to take action but not to dictate whether or what action to take,

---

69 *Id.* at 11.

70 Detection methods could include, but are not limited to: Anomaly Detection, Signature-based detections, Behavioral detections, Indicators of Compromise scanning, Configuration Checking, etc. *See id.* at 12-14.

71 *Id*. at 14.

72 *Id.*

as there may be several factors that an entity needs to consider. Potential actions that could result from the evaluation process might include: (1) escalation following the Responsible Entities incident response plan (as required by Reliability Standard CIP-008); (2) no action; (3) further investigation; (4) tuning of the internal network security monitoring system to reduce false positive notifications or adjust severity level; or (5) other actions as determined by the Responsible Entity, including, for example, whether to involve law enforcement or other external parties.[73]

D. Requirement R2

Proposed Requirement R2 would address the directive in Order No. 887 that Responsible Entities identify anomalous activity to a high level of confidence by maintaining logs and other data collected regarding network traffic.[74] Specifically, Requirement R2 would require each Responsible Entity to implement a process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum, until the evaluation required by Requirement R1, Part 1.3 is complete. Proposed Requirement R2 is shown below:

> **R2.** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3.

Requirement R2 would allow Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time.[75] It is expected that a Responsible Entity's data retention process would

---

73 *Id.*

74 Order No. 887 at P 5.

75 Exhibit C Technical Rationale at 15.

specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all.[76] Regardless of the data retention process created, the goal of the process would be to retain data that can support the analysis required in Requirement R1, Part 1.3. The retention of data would also support a Responsible Entity's incident response and reporting obligation under Reliability Standard CIP-008.[77] Data retention is normally specified by the number of events or records of network communications that are stored in an internal network security monitoring system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an internal network security monitoring system.[78]

E. Requirement R3

Proposed Requirement R3 would address the directive in Order No. 887 that Responsible Entities need to implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.[79] Proposed Requirement R3 would require Responsible Entities to establish one of more processes to protect the internal network security monitoring data collected pursuant to Requirement R1 and data retained pursuant to Requirement R2 from modification or unauthorized deletion by an adversary. Proposed Requirement R3 is shown below:

> **R3.** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

---

76 *Id.*

77 *Id.* An example data retention chart is provided in the Technical Rationale at p. 16.

78 *Id.* at 16.

79 Order No. 887 at P 5.

The processes to protect the internal network security monitoring data collected pursuant to Requirement R1 and data retained pursuant to Requirement R2 would include implementation of protective and detective controls, such as the following: (1) granting only authorized personnel electronic and physical access to the internal network security monitoring system; (2) installing an internal network security monitoring system with built-in methods that safeguard the integrity of stored data; (3) segmenting the internal network security monitoring system into an isolated network separate from the BES Cyber System being monitored; (4) maintaining authentication and authorization systems used by the internal network security monitoring system at a higher assurance level than corporate authentication systems or separated from corporate authentication systems; (5) implementing two-factor authentication for access to the internal network security monitoring system; or (6) utilizing other commonly accepted methods used to protect log data.[80] Requirement R3 would not apply during CIP Exceptional Circumstances, as there may be situations where access may need to be afforded to other individuals supporting a cybersecurity investigation such as additional internal staff, third parties, or government partners.[81]

F. Enforceability

The proposed Reliability Standard also includes measures that support each requirement by clearly identifying what is required and how NERC and the Regional Entities will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear,

---

[80] Exhibit C Technical Rationale at 17.

[81] *See* NERC Glossary of Terms, definition of CIP Exceptional Circumstances, available at: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf. A CIP Exceptional Circumstance is defined as: "A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability."

consistent, and non-preferential manner and without prejudice to any party.[82] Additionally, the proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC and the Regional Entities will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comports with NERC and Commission guidelines related to their assignment. **Exhibit E** provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

As the proposed Reliability Standard incorporates security objectives into requirements, the Compliance Monitoring and Enforcement Program[83] processes and procedures provide effective tools for monitoring and enforcing those security objectives. NERC and the Regional Entities will use existing risk-based compliance monitoring processes to effectively monitor compliance with the new Reliability Standard requirements. As with any new Reliability Standard, NERC and the Regional Entities expect to provide some training and collaboration on the security objectives to ensure that monitoring staff possess the necessary subject matter expertise to employ professional judgment in assessing compliance, consistent with applicable auditing principles.[84] In addition, NERC and the Regional Entities will consider using stakeholder engagement efforts, such as Small Group Advisory Sessions or entity assist visits, as appropriate, to help ensure both Responsible Entities and monitoring staff are prepared for implementation.

---

82 Order No. 672 at P 327.

83 NERC *Rules of Procedure,* Section 400 et. seq.; Appendices 4B and 4C, https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC%20ROP%20effective%2020220825_with%20appendicies.pdf.

84 United States Government Accountability Office, *Government Auditing Standards*, Requirement 3.109 (2024), https://www.gao.gov/assets/d24106786.pdf.

Should a Potential Noncompliance[85] go through enforcement processes for disposition, the existing enforcement processes provide effective means for assessing such findings in a fair and non-preferential manner. For each finding assessed, NERC and the Regional Entities consider the facts and circumstances surrounding each violation and use professional judgment to assess whether security objectives were met, consistent with the FERC-approved Sanction Guidelines.[86] This ensures that enforcement actions bear a reasonable relationship to the seriousness of the violation.[87] In applying such guidelines to requirements with security objectives, NERC and the Regional Entities can follow a repeatable process while ensuring each Responsible Entity is treated fairly based on the unique facts and circumstances of each Potential Noncompliance.

VII. EFFECTIVE DATE OF THE PROPOSED RELIABILITY STANDARDS

NERC respectfully requests that the Commission approve the implementation plan attached to this petition as **Exhibit B**. The proposed implementation plan provides a phased-in approach that is intended to provide protections for the most critical networks (high impact BES Cyber Systems, Control Centers, and backup Control Centers) more quickly while recognizing the significant work that needs to be completed to fully implement the CIP-015-1 requirements.

The proposed implementation plan would have the proposed Reliability Standard become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective

---

[85] *See* NERC *Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure* (effective May 19, 2022) at 17 ("Potential Noncompliance" means the identification, by the Compliance Enforcement Authority, of a possible failure by a Registered Entity to comply with a Reliability Standard that is applicable to the Registered Entity); https://www.nerc.com/AboutNERC/RulesOfProcedure/ROP_Appendix%202_20220519.pdf.

[86] *See* NERC *Sanction Guidelines of the North American Electric Reliability Corporation* (effective January 19, 2021) at 3; https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_4B_effective%2020210119.pdf.

[87] *Id.*

date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1 Parts 1.1 and 1.2 would be required to initially comply with the requirements in proposed CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe would recognize the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It would further accommodate for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of internal network security monitoring.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers, would be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation would allow for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers that pose the greatest risk to reliability. It would further balance the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets. As such, the proposed implementation plan for Reliability

Standard CIP-015-1 balances the urgency in the need to implement the standard against the time needed to comply.[88]

VIII. CONCLUSION

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

- Proposed Reliability Standard CIP-015-1, and the associated elements, as shown in **Exhibit A;** and
- The implementation plan included in **Exhibit B**.

Respectfully submitted,

/s/ Sarah P. Crawford

Lauren A. Perotti
Assistant General Counsel
Sarah P. Crawford
Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
lauren.perotti@nerc.net
sarah.crawford@nerc.net

Counsel for the North American Electric Reliability Corporation

June 24, 2024

[88] *See* Order No. 672, at P 333 ("In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit A

Proposed Reliability Standard CIP-015-1

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024
20-day formal comment period with ballot	02/27/2024 – 03/18/2024
10-day formal comment period with ballot	04/05/2024 – 04/17/2024

Anticipated Actions	Date
7-day final ballot	04/24/2024 – 04/30/2024
Board adoption	TBD

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 – Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but is not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1 (1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s) (1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.
R2.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented

				process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.
R3.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC)[2]. INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address three security issues.

[1] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] *Id.* P 5. (Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment) and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices).

In Order No. 887, FERC directs NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

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 thirty-six (36) 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.

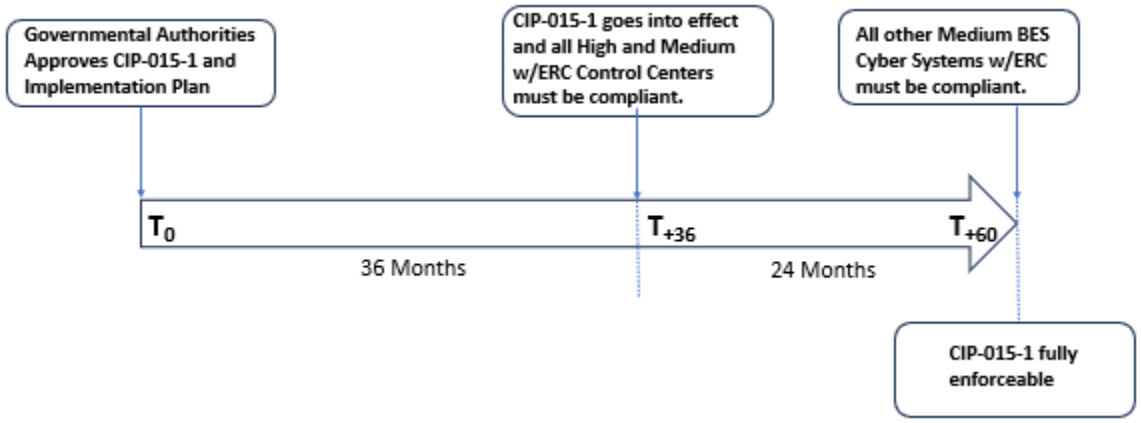
Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1 Parts 1.1. and 1.2. shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It

further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit C

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address three security objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of networks that are internal to the

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following three security objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

operational zones of the Responsible Entity. While the Responsible Entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices that are protected by the ESP of applicable BES Cyber Systems.

Reliability Standard CIP-015-1 requires Responsible Entities to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to anomalous network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation could include escalation to a Responsible Entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. INSM will be an on-going, or possibly an iterative, process enabling Responsible Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887, schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Creation of new Standard CIP-015

At the start of Project 2023-03 – INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In

[3] NERC Glossary of Terms
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with the DT's objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting

reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification
The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM
The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.*

Summary
Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the Responsible Entity for network monitoring purposes.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications."

As described in Richard Bejtlich's book, "The Practice of Network Security Monitoring", monitoring is most effective when collection is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods (Chapters 9-11). In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein Responsible Entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1. specifies that the Responsible Entity identify possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ESP networks and select and implement one or more INSM network data feed(s) in each ESP. These data feeds provide the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.

Network Data Feeds

A network data feed is the combination of a data collection location and a data collection method. Collection methods are technologies that provide visibility of network data to an INSM system (examples are provided below). In context of Reliability Standard CIP-015-1, network locations are physical or virtual devices that move data on a network. These devices include switches, virtual switches, firewalls, routers, network interfaces and similar devices.

Data Collection Locations

Data collection locations may be a physical or a logical concept. In a physical context, network data collection locations connote data collection from devices that move data within and between networks such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. A Responsible Entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the

Responsible Entity may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments.

	High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Considerations for selecting Network Data Feeds

The following considerations might inform the decision for collecting data from a network data feed:

Adversary Analysis

The Responsible Entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive network data feeds that focus on targeted uses cases.

ICS Protocols

The network data feeds, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyze ICS specific protocols.

Data Types

The MITRE ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting network data feeds, a Responsible Entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network data feeds. Consideration of traffic duplication may be part of a rationale on how network data feeds were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data feeds.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network data feeds were selected or excluded for data collection.

A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Parts 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alerts in some INSM systems. Suppressing alarms or data collection may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.
2. High rates of false positive alerts until tuning can be completed.
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the DT these common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

Partner Networks

Transmission Operators have connections to partner networks for the purpose of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some Generator Operators implement connections to external partners for turbine monitoring systems. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value for INSM data collection.

Resilience
While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1. allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN
Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering
Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection
Requirement R1, Part 1.1. does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability
Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a “per system capability” exclusion, Requirement R1, Part 1.1. allows wide latitude to identify INSM network data feeds appropriate to each Responsible Entity’s ESP networks.

Some networks may not have the capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity has several options to provide monitoring data to the INSM including:

- Upgrading hardware and software to systems that do have the capability.
- Installing TAPs to collect network data.

- Collecting flow data.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity.
- Supplementing network data feeds with other pertinent data feeds such as endpoint logs and firewall logs.
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[6].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities are not expected to implement all of these, but rather to choose and implement the network data feeds that provide the most value to the Responsible Entity, as determined by the risk-based rationale in Requirement R1, Part 1.1.

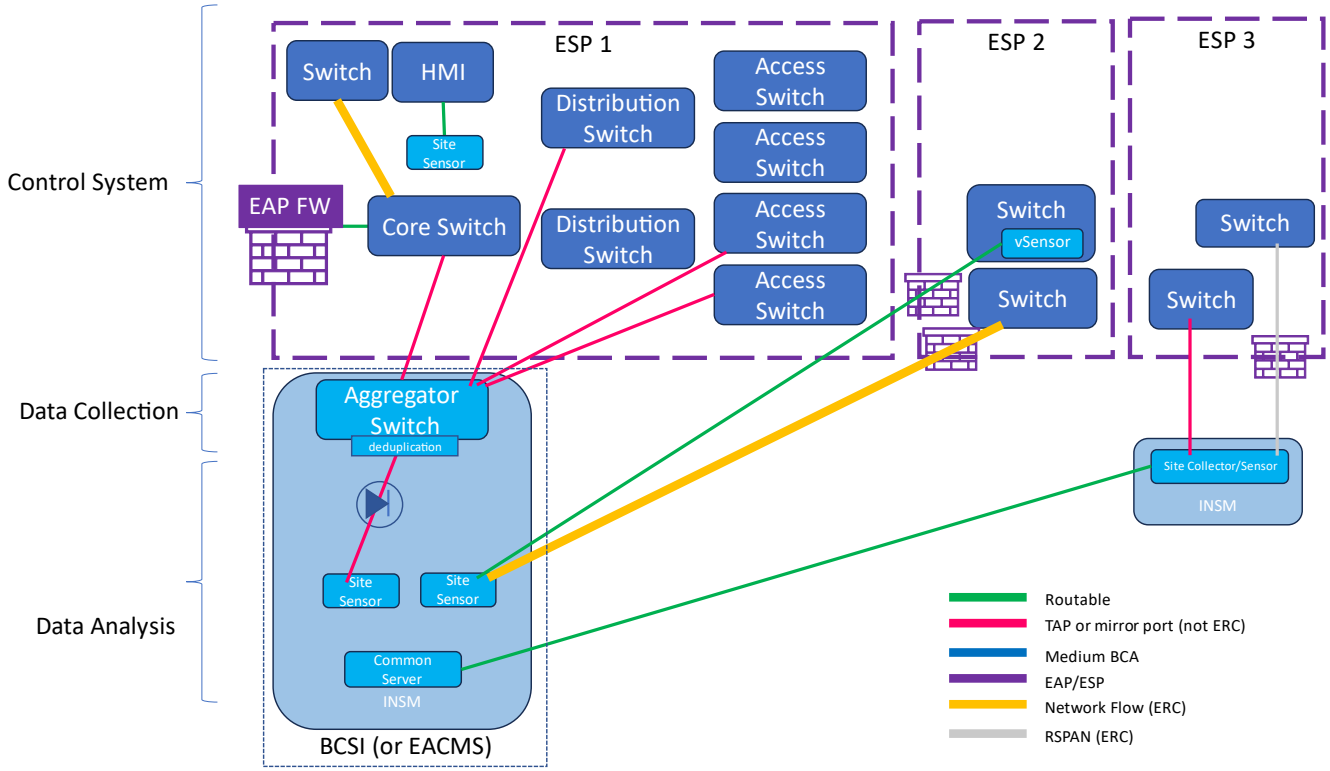


Figure 1

[6] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

This reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new or modified Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of technology advancements, new anomalous detection products are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and INSM Requirement R1 and Requirement R1, Part 1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

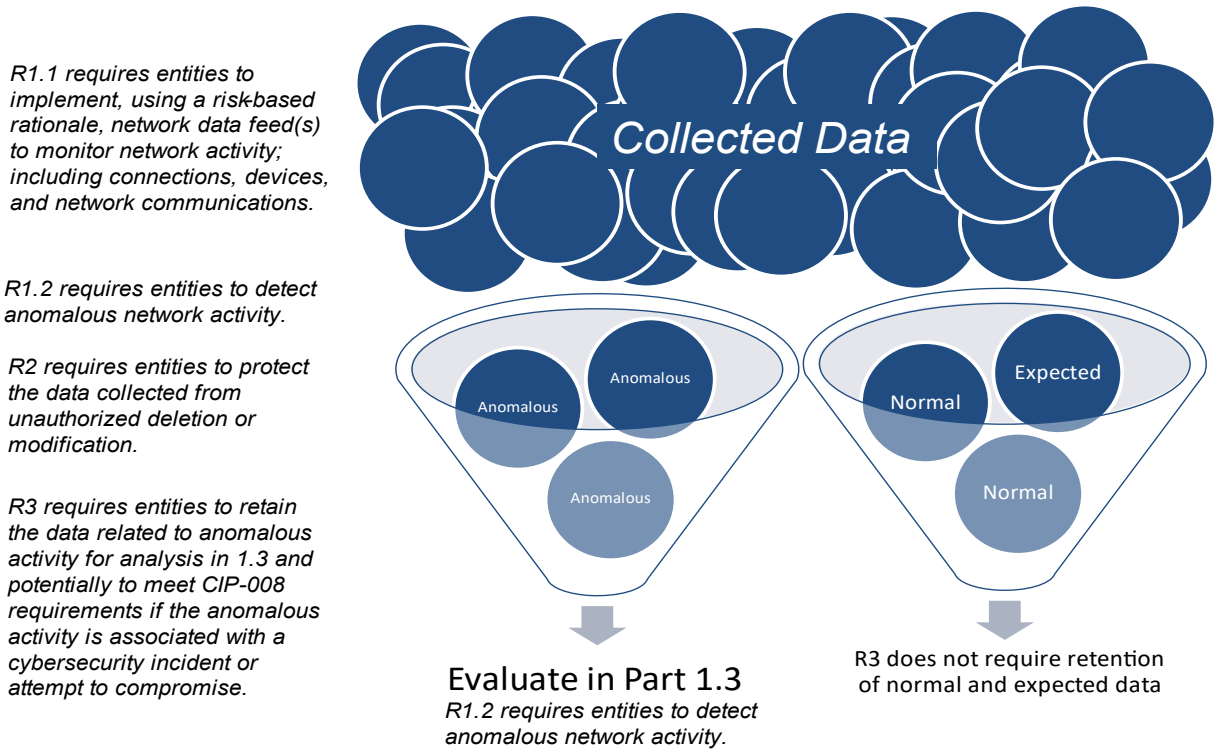


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected

traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Signature-based detections
Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.
When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for data retention in Requirement R3.

Behavioral Detections
Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[7] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning
After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking
INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods
Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods
As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

[7] https://attack.mitre.org/techniques/T0888/

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).
- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning
Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3. "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[8] book. Analyzing the data is an expected part of cyber security operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[8] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

Rationale for Requirement R2

Requirement R2: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3."

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Requirement R2 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide evidence needed to meet CIP-008-6 Requirement R2 for data retention related to an actual Cyber Security Incident or attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system.

Rationale for Requirement R3

Requirement R3: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[9]). The intent of Requirement R3 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system.
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement R3 is intended to limit information sharing. The focus of Requirement R3 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities to share information gathered by INSM systems (see NIST 800-150[10], CISA Information Sharing Guidance[11], Cyber security Information Sharing act of 2015[12]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[13]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities may

[9] https://attack.mitre.org/techniques/T1070/
[10] https://csrc.nist.gov/pubs/sp/800/150/final
[11] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[12] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[13] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf See Page 8

need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feeds to implement as part of Requirement R1, Part 1.1.

The table below uses the following simplified diagram of a high impact ESP network.

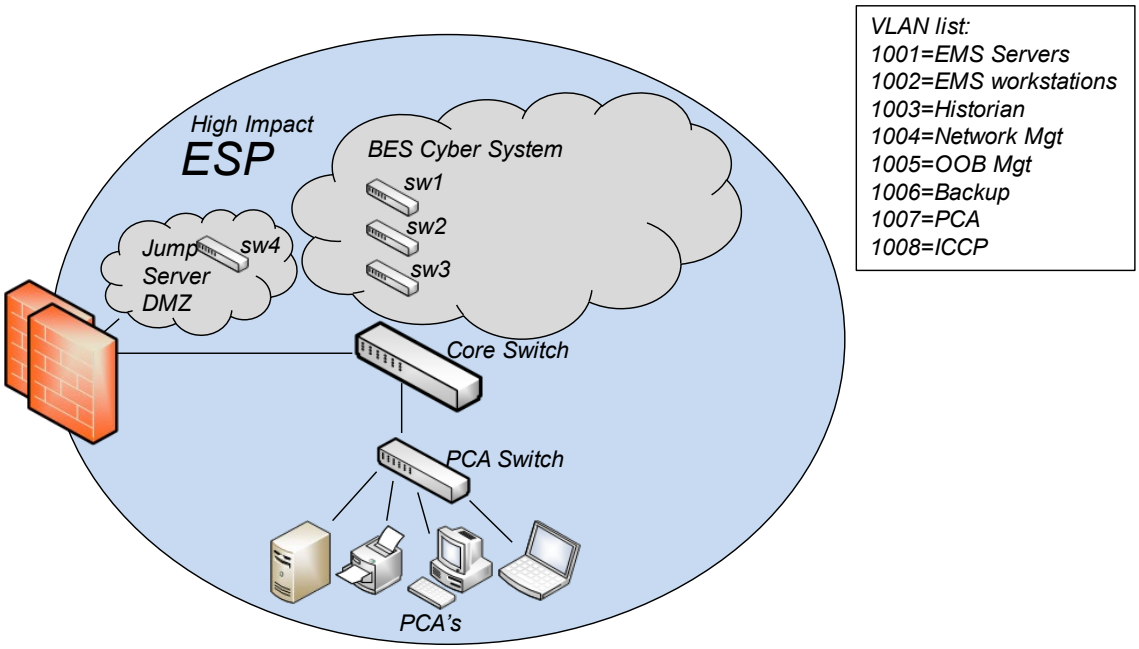


Figure 3

Example rationale for selecting Network Data Feeds:

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports	IRA to the jump server is a likely attack vector.

			to physical port	
	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected

				to be abused by a malicious insider. The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.
Firewall Log data	Yes	Firewall	API	The INSM tool includes a built-in integration to the firewall which provides information about blocked connection attempts.

This example provides some of the considerations for selecting network data feeds. This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.

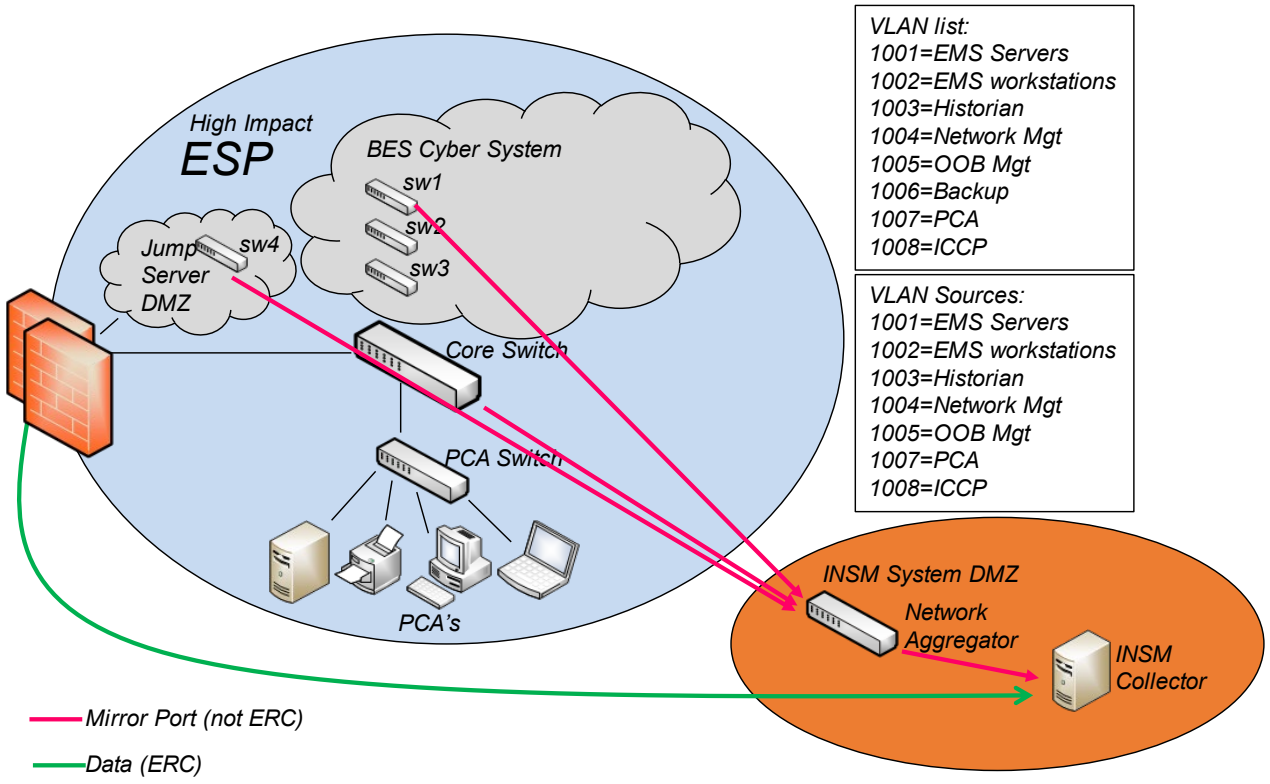

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.
V0.3	24 Apr 2024	Changes based on industry comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit D

Order No. 672 Criteria

EXHIBIT D

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standard meets or exceeds 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 Standard improves upon and expands the protections required by NERC's CIP Reliability Standards by establishing requirements for internal network security monitoring for network traffic inside an Electronic Security Perimeter ("ESP"). Such monitoring would improve the probability of detecting anomalous or unauthorized network activity, thus facilitating an improved response to and recovery from an attack. Specifically, Responsible Entities would evaluate their networks within Electronic Security Perimeters and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities would then be required to collect, analyze, and respond appropriately to anomalous network communications within applicable networks. Responsible Entities would also be required to evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. In addition, proposed Reliability Standard CIP-015-1 would require Responsible Entities to protect the collected internal network security monitoring related network communications data to prevent unauthorized data manipulation and

---

[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, *supra* note 1, at P 324.

preserve the data as needed to facilitate additional investigation. Proposed Reliability Standard CIP-015-1 would advance the reliability of the Bulk-Power System ("BPS") by providing a comprehensive suite of requirements for internal network security monitoring, that are forward looking and objective-based, consistent with Order No. 887.[3]

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.[4]

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standard applies to Balancing Authorities, Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standard clearly articulates 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.[5]

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

---

[3] *See Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023).
[4] *See* Order No. 672, *supra* note 1, at PP 322, 325.
[5] *See* Order No. 672, *supra* note 1, at P 326.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner.[6]

The proposed Reliability Standard contains 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.

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.[7]

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

6. Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[8]

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. Proposed Reliability Standard CIP-015-1 would advance the reliability of the BPS by providing a comprehensive suite of requirements for internal network security monitoring, that are forward looking and objective-based, consistent with the directives set forth in Order No. 887.[9]

---

[6] *See* Order No. 672, *supra* note 1, at P 327.
[7] *See* Order No. 672, *supra* note 1, at P 328.
[8] *See* Order No. 672, *supra* note 1, at PP 329-30.
[9] *See Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023).

The proposed Reliability Standard would require Responsible Entities to evaluate their networks within Electronic Security Perimeters and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities would then be required to collect, analyze, and respond appropriately to anomalous network communications within applicable networks. Responsible Entities would also be required to evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. In addition, proposed Reliability Standard CIP-015-1 would require Responsible Entities to protect the collected internal network security monitoring related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation.

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.[10]

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

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[11]

The proposed Reliability Standard has no undue negative impact on competition. The proposed Reliability Standard requires the same performance by each of the applicable Functional Entities for mitigating the risks posed by loss of availability and communication links used for Real-time Assessment and Real-time monitoring data while such data is being transmitted between

[10] *See* Order No. 672, *supra* note 1, at P 331.
[11] *See* Order No. 672, *supra* note 1, at P 332.

any applicable Control Centers. The proposed Reliability Standard does not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[12]

The proposed implementation period for the proposed Reliability Standard is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply. The proposed implementation plan provides a phased-in approach that is intended to provide protections for the most critical networks (high impact BES Cyber Systems, Control Centers, and backup Control Centers) more quickly while recognizing the significant work that needs to be completed to fully implement the CIP-015-1 requirements.

The proposed implementation plan would have the proposed Reliability Standard become effective on the first day of the first calendar quarter that is thirty-six (36) 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. All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1 Parts 1.1 and 1.2 would be required to initially comply with the requirements in proposed CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe would recognize the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It would further accommodate for the challenges posed by the limited pool of vendors,

[12] *See* Order No. 672, *supra* note 1, at P 333.

time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of internal network security monitoring.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers would be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[13]

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved processes for developing and approving Reliability Standards. Exhibit F includes a summary of the development proceedings and details the processes followed to develop the proposed Reliability Standard. These processes included, among other things, comment and ballot periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum, and 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.[14]

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

12. Proposed Reliability Standards must consider any other appropriate factors.[15]

---

[13] *See* Order No. 672, *supra* note 1, at P 334.
[14] *See* Order No. 672, *supra* note 1, at P 335.
[15] *See* Order No. 672, *supra* note 1, at P 323.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit E

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es). Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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	The proposed VSL is binary. It does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-015-1, Requirement R2	
Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSL is binary. It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit F

Summary of Development History and Complete Record of Development

Summary of Development History

The following is a summary of the development record for proposed Reliability Standard CIP-015-1.

I. Overview of the 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 drafting team selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the drafting team consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2023-03 drafting team members is included in **Exhibit G**.

II. Standard Development History

A. Federal Energy Regulatory Commission Directive

Project 2023-03 Internal Network Security Monitoring ("INSM") addresses FERC Order No. 887[3] directing NERC to develop requirements within the Critical Infrastructure Protection ("CIP") Reliability Standards for internal network security monitoring of all high impact Bulk Electric System ("BES") Cyber Systems with or without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.

B. Standard Authorization Request Development

On March 22, 2023, the Standards Committee authorized posting a Standards Authorization Request ("SAR") proposing to develop requirements for internal network security

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2018).

2 The NERC *Standard Processes Manual* is available at https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_3A_SPM_Clean_Mar2019.pdf.

3 *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023).

monitoring for all high impact BES Cyber Systems and those medium impact BES Cyber Systems with external routable connectivity for a 30-day informal comment period from April 6, 2023 through May 5, 2023 and authorized the solicitation of drafting team members.[4] The Standards Committee accepted the SAR on August 23, 2023.

C. First Posting - Comment Period, Initial Ballot, and Non-binding Poll

On August 23, 2023, the Standards Committee approved a waiver under Section 16.0 of the Standard Processes Manual to shorten the usual periods for comment and ballot for Project 2023-03. Specifically, the Standards Committee approved shortening the initial formal comment and ballot period from 45 days to as little as 30 days, with ballot pools formed in the first 20 days and ballots conducted in the last 5 days, shortening the additional formal comment and ballot period(s) from 45 days to as little as 20 days with ballot conducted during the last 5 days; and shortening the final ballot from 10 days to as little as 5 days.[5]

On December 13, 2023, the Standards Committee authorized the initial posting of proposed Reliability Standard CIP-007-X and the associated Implementation Plan and other associated documents for a 35-day formal comment period.[6] The initial posting took place from December 14, 2023 through January 17, 2024 with a parallel initial ballot and non-binding poll on the Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") held during the last 10

---

[4] *See* NERC Standards Committee March 22, 2023 Agenda Package, Agenda Item 7, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Agenda_Package_March%2022_2023.pdf.

[5] *See* NERC Standards Committee August 23, 2023 Meeting Minutes at 1-2, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/August%20Meeting%20Minutes%20-%20Approved%20September%2020,%202023.pdf.

[6] *See* NERC, Standards Committee December 23, 2023 Meeting Minutes at 4, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20December%20Minutes%20-%20Approved%20January%2017,%202024.pdf

days of the comment period from January 8, 2024 through January 17, 2024.[7] The initial ballot for proposed Reliability Standard CIP-007-X received 15.42 percent approval, reaching quorum at 82.03 percent of the ballot pool, and the initial ballot for the associated Implementation Plan received 44.89 percent approval reaching quorum at 83.86 percent of the ballot pool.[8] The non-binding poll for the associated VRFs and VSLs received 11.98 percent supportive opinions, reaching quorum at 84.4 percent of the ballot pool.[9] There were 75 sets of responses, including comments from approximately 198 different individuals and approximately 116 companies, representing all 10 industry segments.[10]

D. Standards Committee Authorizes Procedural Waiver and Creation of New Standard

On January 31, 2024, following a review of the comments from the January 2024 initial ballot for proposed Reliability Standard CIP-007-X, the drafting team voted to create a new CIP Standard, Reliability Standard CIP-015-1, rather than modify CIP-007-X.[11] The Standards Committee also authorized a waiver of Sections 4.9 and 4.12 of the Standard Processes Manual to reduce the additional formal comment and ballot periods for Project 2023-03 from 45 days to as little as 10 calendar days, with ballot conducted during the last five days of the comment period.[12]

---

7 *See* Exhibit F, Complete Record of Development, at item 17.

8 *Id.* at items 23, 24.

9 *Id.* at item 25.

10 *Id.* at item 10.

11 *See* NERC Standards Committee February 21, 2024 Agenda Package, Agenda Item 5, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Meeting_Agenda_February_21_2024%201.pdf.

12 *See* NERC Standards Committee Meeting Agenda March 20, 2024, Agenda Item 2a – Meeting Minutes-February 2024, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Meeting_Agenda_March_20_2024.pdf

E. Second Posting - Comment Period, Additional Ballot, and Non-binding Poll

The first draft of proposed Reliability Standard CIP-015-1, the associated Implementation Plan, and other associated documents were posted for a 20-day formal comment period from February 27, 2024 through March 18, 2024, with a parallel additional ballot and non-binding poll held from March 12, 2024 through March 18, 2024.[13] The additional ballot for proposed Reliability Standard CIP-015-1 received 48.52 percent approval, reaching quorum at 91.02 percent of the ballot pool, and the additional ballot for the associated Implementation Plan received 66.71 percent approval with 91.34 percent quorum.[14] The non-binding poll for the associated VRFs and VSLs received 47.54 percent supportive opinions, reaching quorum at 88.66 percent of the ballot pool.[15] There were 73 sets of responses, including comments from approximately 160 different individuals and approximately 102 companies, representing 7 industry segments.[16]

F. Third Posting – Comment Period, Additional Ballot, and Non-binding Poll

The second draft of proposed Reliability Standard CIP-015-1, the associated Implementation Plan, and other associated documents were posted for a 13-day formal comment period from April 5, 2024 through April 17, 2024, with a parallel additional ballot and non-binding poll held from April 12, 2024 through April 17, 2024.[17] The additional ballot for proposed Reliability Standard CIP-015-1 received 76.78 percent approval reaching quorum at 90.63 percent of the ballot pool, and the additional ballot for the associated Implementation Plan received 80.69 percent approval with 90.55 percent quorum.[18] The non-binding poll for the associated VRFs and

---

13 *See* Exhibit F, Complete Record of Development at item 35.

14 *Id.* at items 40,41.

15 *Id.* at item 42.

16 *Id.* at item 36.

17 *Id.* at item 53.

18 *Id.* at items 58, 59.

VSLs received 79.56 supportive opinions, reaching quorum at 88.26 percent of the ballot pool.[19] There were 55 sets of responses, including comments from approximately 142 different individuals and approximately 87 companies, representing all 10 industry segments.[20]

G. Final Ballot

The final draft of proposed Reliability Standard CIP-015-1 was posted for a 7-day final ballot period from April 24, 2024 through April 30, 2024.[21] The final ballot for proposed Reliability Standard CIP-015-1 reached quorum at 93.36 percent of the ballot pool, receiving support from 76.57 percent of the voters.[22] The ballot for the Implementation Plan reached quorum at 93.31 percent of the ballot pool, receiving support from 82.1 percent of the voters.[23]

H. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standard CIP-015-1 on May 9, 2024.[24]

---

19 *Id.* at item 60.

20 *Id.* at item 54.

21 *Id.* at item 72.

22 *Id*. at item 73.

23 *Id*. at item 74.

24 NERC, *Board of Trustees Agenda Package May 9, 2024*, Agenda Item 5c. (Project 2023-03 Internal Network Security Monitoring), https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board%20of%20Trustees%20Agenda%20Package%20-%20May%209%202024.pdf.

Complete Record of Development

Project 2023-03 Internal Network Security Monitoring (INSM)

Related Files

Status

Board Adopted: May 9, 2024

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for internal network security monitoring (INSM) of all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic once it is within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements that are "forward-looking, objective-based"[2] and address three security objectives outlined in Order No. 887. FERC directed NERC to submit these revisions for approval by July 9, 2024.

Standard(s) Affected: CIP-015-1

Purpose/Industry Need

While the CIP Reliability Standards require monitoring of the Electronic Security Perimeter and associated systems for high and medium impact Bulk Electric System (BES) Cyber Systems, the CIP networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This presents a gap in the currently effective CIP Reliability Standards. To address this gap, CIP Reliability Standards should be created or modified to require INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack. Current CIP Reliability Standards are insufficient to protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds.

Subscribe to this project's observer mailing list

Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2023-03 Internal Network Security Monitoring Observer List" in the Description Box.

[1] Internal Network Security Monitoring for High and Medium Impact Bulk electric System Cyber Systems, Order No. 887, 182 FERC ¶ 61,021 (Jan. 19, 2023).

[2] Order No. 87 at P 5.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft **CIP-015-1** **(61)** Clean | **(62)** Redline | **(63)** Redline of R2, R3, M2, and M3 language *Please Note: The DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline. **Implementation Plan** **(64)** Clean | **(65)** Redline **Supporting Materials** **VRF/VSL Justifications** **(66)** Clean | **(67)** Redline **Technical Rationale** **(68)** Clean | **(69)** Redline **FAQ for CIP-015-1** **(70)** Clean | **(71)** Redline	Final Ballot **(72)** Info Vote	04/24/24- 04/30/24	Ballot Results **(73)** CIP-015-1 **(74)** Implementation Plan	
Additional Ballot, Draft 2 of **CIP-015-1** **(43)** Clean | **(44)** Redline *updated Requirement R1 was updated to correct an error in the language from "BES Security Systems" to "BES Cyber Systems" to align with the clean version of Draft 2 of CIP-015-1. **Implementation Plan** **(45)** Clean | **(46)** Redline **Supporting Materials** **(47)** Unofficial Comment Form **VRF/VSL Justifications** **(48)** Clean | **(49)** Redline **Technical Rationale** **(50)** Clean | **(51)** Redline **(52)** FAQ for CIP-015-1	Additional Ballot **(56)** Ballots Open Reminder **(57)** Info*updated Vote	04/12/24- 04/17/24	Ballot Results **(58)** CIP-015-1 **(59)** Implementation Plan Non-Binding Poll Result **(60)** CIP-015-1	
	Comment Period **(53)** Info Submit Comments	04/05/24- 04/17/24	**(54)**Comments Received	**(55)** Consideration of Comments

Additional Ballot, Draft 1 of **CIP-015-1** **(27)** Clean **CIP-007-X** **(28)** Redline Based on comments received, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. The files above reflect the new CIP-015-1 and removal of Requirement R6 and its parts from CIP-007-X. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. **Implementation Plan** **(29)** Clean | **(30)** Redline **Supporting Materials** **(31)** Unofficial Comment Form **VRF/VSL Justifications** **(32)** Clean | **(33)** Redline **(34)** Technical Rationale	Initial Ballot of CIP-015 (additional ballot for the Project 2023-03) **(38)** Ballots Open Reminder **(39)** Info Vote	03/12/24- 03/18/24	Ballot Results **(40)** CIP-015-1 **(41)** Implementation Plan Non-Binding Poll Result **(42)** CIP-015-1	**(37**Consideration of Comments
	Comment Period **(35)** Info Submit Comments	02/27/24- 03/18/24	**(36)**Comments Received	
	Ballot Pools The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.			
(26) Waiver	Standards Committee accepted the waiver on February 21, 2024.			
Draft 1 **CIP-007-X** **(11)** Clean | **(12)** Redline **(13)** Implementation Plan **Supporting Materials** **(14)** Unofficial Comment Form **(15)** VRF/VSL Justifications **(16)** Technical Rationale	Initial Ballot **(21)** Ballots Open Reminder **(22)** Info Vote	01/08/24- 01/17/24	Ballot Results **(23)** CIP-007-X **(24)** Implementation Plan Non-Binding Poll Result **(25)** CIP-007-X	
	Join Ballot Pools **(20)** Ballot Pools Forming Reminder	12/14/23 - 01/02/24	**(18)** Comments Received	**(19)** Consideration of Comments
	Comment Period **(17)** Info Submit Comments	12/14/23 - 01/17/24		
Waiver **(9)** Waiver **(10)** Meeting Minutes	Standards Committee accepted the waiver on August 23, 2023.			
Standard Authorization Request (SAR) **(7)** Clean | **(8)** Redline	The Standards Committee accepted the SAR on August 23, 2023			
Drafting Team Nominations **Supporting Materials** **(5)** Unofficial Nomination Form (Word)	Nomination Period **(6)** Info Submit Nominations	04/06/2023 – 05/05/2023		
(1)Standard Authorization Request **Supporting Materials** **(2)** Unofficial Comment Form (Word)	Comment Period **(3)** Info Submit Comments	04/06/2023 – 05/05/2023	**(4)** Comments Received	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

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:	Internal Network Security Monitoring (INSM)		
Date Submitted:	March 7, 2023		
SAR Requester			
Name:	Michaelson Buchanan, Dan Goodlett, Larry Collier		
Organization:	NERC		
Telephone:	470.725.5268, 470.522.7367, 470.716.2923	Email:	Michaelson.buchanan@nerc.net Dan.goodlett@nerc.net Larry.Collier@nerc.net
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 the CIP Reliability Standards require monitoring of the Electronic Security Perimeter and associated systems for high and medium impact Bulk Electric System (BES) Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This presents a gap in the currently effective CIP Reliability Standards. To address this gap, CIP Reliability Standards should be created or modified to require INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack. Current CIP Reliability Standards are insufficient to protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
As directed by FERC Order No. 887, modify or create new Standard(s) that require INSM within a trusted Critical Infrastructure Protection networked environment for all high impact BES Cyber Systems with and without ERC and medium impact BES Cyber Systems with ERC.
Project Scope (Define the parameters of the proposed project):
The Standard Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order. The scope of the project will include: • All high impact BES Cyber Systems, and • All medium impact BES Cyber Systems with ERC The scope of the project should not extend to: • medium Impact BES Cyber Systems without ERC or • low impact BES cyber systems The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.
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):
Create new or modified existing CIP Reliability Standards that are forward-looking, objective-based, and that address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment. And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by: (1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

[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.

Requested information
Beyond the time and resources needed to serve on the Standard Drafting Team, the cost to entities will vary based on their current system architecture. While many entities may have the controls in place, others may not which could require a significant cost investment depending on their footprint.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None.
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):
Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Interchange Coordinator, Interchange Authority, Reliability Coordinator, Transmission Operator, Transmission Owner
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.
The SAR has been developed in response to FERC Order No. 887. The final Order was consistent with feedback provided by NERC and industry through the NOPR process. NERC and the ERO Enterprise have convened a response team to address directives in the FERC Order which included a review of this SAR.
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)?
The following projects and Reliability standards should be assessed for impact: • Projects 2016-02, 2019-03 and 2022-05 • Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2
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.
This Standards Authorization Request has been developed pursuant to FERC Order No. 887.

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.

[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.

Reliability Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

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
N/A	

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
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-03 Internal Network Security Monitoring (INSM)

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2023-03 Internal Network Security Monitoring** Standard Authorization Request (SAR) by **8 p.m. Eastern, Friday, May 5, 2023.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Laura Anderson (via email), or at 404-782-1870.

Background Information

The proposed project will address the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic once it is within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity.

More specifically, Order No. 887 directs NERC to develop Reliability Standards requirements that are "forward-looking, objective-based"[2] and address three security objectives outlined in Order No. 887. FERC directed NERC to submit these revisions for approval by July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, all low impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC is conducting the study, which is to be filed with FERC by January 18, 2024.

[1] Internal Network Security Monitoring for High and Medium Impact Bulk electric System Cyber Systems, Order No. 887, 182 FERC ¶ 61,021 (Jan. 19, 2023).
[2] Order No. 87 at P 5.

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 2023-03 Internal Network Security Monitoring (INSM) Standard Authorization Request

Informal Comment Period Open through May 5, 2023

Now Available

A 30-day informal comment period for the **Project 2023-03 Internal Network Security Monitoring** Standard Authorization Request (SAR), is open through **8 p.m. Eastern, Friday, May 5, 2023.**

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

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, Laura Anderson (via email) or at 404-446-9671. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | SAR
Comment Period Start Date:	4/6/2023
Comment Period End Date:	5/5/2023
Associated Ballots:	

There were 37 sets of responses, including comments from approximately 114 different people from approximately 88 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
WEC Energy Group, Inc.	Christine Kane	3,4,5,6		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Tacoma Public Utilities (Tacoma, WA)	Jennie Wike	1,3,4,5,6	WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	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
MRO	Jou Yang	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Chris Bills	City of Independence, Power and Light Department	5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern	1	MRO

						Power Administration		
					Matthew Harward	Southwest Power Pool, Inc. (RTO)	2	MRO
					Bryan Sherrow	Board of Public Utilities	1	MRO
					Terry Harbour	Berkshire Hathaway Energy - MidAmerican Energy Co.	1	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Shonda McCain	Omaha Public Power District	6	MRO
					George E Brown	Pattern Operators LP	5	MRO
					George Brown	Acciona Energy USA	5	MRO
					Jaimin Patel	Saskatchewan Power Cooperation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jay Sethi	Manitoba Hydro	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy -	5	RF

						FirstEnergy Solutions		
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) Project 2023-03 INSM SAR	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Elizabeth Davis	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
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
					Jim Howell, Jr.	Southern Company - 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 RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					John Pearson	ISO New England, Inc.	2	NPCC
					Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
					Randy MacDonald	New Brunswick Power Corporation	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power	1	NPCC

						Authority		
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
NiSource - Northern Indiana Public Service Co.	Steve Toosevich	1,3,5,6		NIPSCO Compliance	Steven Taddeucci	NiSource - Northern Indiana Public Service Co.	3	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Joseph OBrien	NiSource - Northern Indiana Public Service Co.	6	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.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer	No
Document Name	

Comment

PNM does not agree with the proposed scope as described in the SAR.

While PNM agrees that Internal Network Security Monitoring (INSM) for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) is important, it is unclear what “forward-looking, objective based” requirements are or would look like without understanding what the specifics of these requirements would be. PNM is hesitant that Standards geared toward implementing INSM controls could become more prescriptive in nature instead of offering guidance on allowable models and controls for entities to consider in determining INSM models for their specific and unique environments.

Order No. 887 refers to a zero-trust architecture as being “fundamental” in INSM. PNM agrees but requests clarity on the definition and scope of zero-trust as it would function in meeting INSM requirements. Zero trust could refer to good network segmentation. It could also refer to a more comprehensive re-building of a network from scratch. The scope of this project could vary greatly depending on industry interpretation of and the necessity to use a zero-trust environment.

PNM also agrees with the comments put forth by EEI that if new requirements were to be put in place, they would need to be risk-based.

Likes 0	
Dislikes 0	

Response

Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The MRO NSRF suggests the detailed description section be modified with additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text:

“First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment.”

The use of the term “baseline” could restrict the choice of a vendor based on how their technology was implemented. The associated compliance

evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity. The MRO NSRF suggests the following wording:

"First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model."

The detailed description provides a list of required detections:

"Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment."

The MRO NSRF requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010.

The following text is suggested:

"Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use"

The detailed description also contains the following scoping requirement:

"And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by…"

The MRO NSRF suggests that the term "to a high level of confidence" be removed. In a zero-defect compliance environment, the requirement to prove a high level of confidence is difficult as it is a subjective statement.

The MRO NSRF suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid duplicating requirements. It is unclear why CIP-013 is included in the SAR, the MRO NSRF asks for additional clarity in the SAR, if in fact CIP-013 is to

remain in the SAR scope	
Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed scope in the SAR. Below is a summary of Tacoma Power's recommended changes to the SAR scope.

1. Tacoma Power recommends deleting the following bolded language from the last sentence in the Industry Need section in the SAR: "Current CIP Reliability Standards are insufficient to protect against insider threats **or vulnerabilities that are exploited through supply chain attacks such as SolarWinds**." The CIP Standards did protect against the SolarWinds supply chain attack, because the Requirements were sufficient to prevent this attack from affecting the BES reliability. Tacoma Power is concerned that the wording of this SAR implies there were BES reliability impacts from the SolarWinds event. Additionally, the INSM Requirements would provide more protections for threats beyond supply chain, so this statement is not necessary.
2. Tacoma Power proposes that the scope of Project 2023-03 be limited to medium impact BES Cyber Systems at a Control Center. Inbound and outbound malicious communication detection is not yet required in CIP-005 for medium impact BES Cyber System with ERC. INSM is also easier to implement in a Control Center environment than a substation. If FERC Order 887 requires detection of malicious communication at substations, then Tacoma Power recommends that this detection be limited to inbound and outbound detection instead of INSM. This SAR is proposing to skip the step of developing new CIP-005 R1.5 Requirements for inbound and outbound malicious communication detection for medium impact BES Cyber Systems with ERC, and immediately implement INSM.
3. In the Detailed Description section of the SAR, Tacoma Power is concerned with the following numerical items: "(1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices." These three items are not sufficient on their own to implement an INSM. For example, logging network traffic doesn't support INSM. Tacoma Power recommends deleting these three items.If the Detailed Description remains as written, Tacoma Power recommends that the Detailed Description be expanded to include a description of the objective of capturing and storing the logged data. Ultimately, the objective of INSM is that entities have a process to detect malicious activity inside the CIP network.
4. Tacoma Power recommends deleting Interchange Coordinator and Interchange Authority from the Applicability section of the SAR, as follows: "Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner"

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	No
Document Name	

Comment
FE supports EEI's comments and would recommend CIP-008 for inclusion in the scope of this project.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No
Document Name	

Comment
The scope of the SAR describes the objectives well and contains good details. Manitoba Hydro suggests the detailed description section be modified with some additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text: "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment." The use of the term "baseline" could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity. Manitoba Hydro suggests the following wording: "First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model." The detailed description provides a list of required detections: "Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment." Manitoba Hydro requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010. The following text is suggested: "Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use" Manitoba Hydro suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid

duplicating requirements. It is unclear why CIP-013 is included in the SAR, Manitoba Hydro asks for additional clarity in the SAR, if in fact CIP-013 is to remain in the SAR scope.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI agrees with the intended scope of the SAR, however, some of the language used in this SAR, while closely aligned with the language in FERC Order 887, does not align with the scoping language for a NERC Reliability Standard. To address these concerns, we offer the following:

1. Project Scope Section: The last sentence in this section should be deleted because it adds no additional insights or direction to the SDT regarding the project scope. Moreover, the scope of the Commission's directives are clear and concise. This sentence in the SAR is a directive for NERC and outside the scope for this project.
2. Detailed Description Section: While the language contained in this section closely aligns with the Commission's Directives, changes are necessary to ensure the directions provided to the SDT are clear, unambiguous and align with NERC's Results Based Standards processes. We additionally note that while we did not delete the phrase "**to a high level of confidence**" in our suggested changes to the Detailed Description section, we do not support changes to the Reliability Standard that are not risk-based. Our proposed changes are as identified in boldface below (deletions not shown because SBS does not accept strikethrough text):

Detail Description Section: Create new or modified CIP Reliability Standards that are **risk**-based and address the need for responsible entities to **utilize security processes, systems and tools that 1)** develop baselines of network traffic inside **an Electronic Security Perimeter; 2)** monitor **for** and detect unauthorized activity, connections, devices, and software inside **an Electronic Security Perimeter; 3) are capable of** identify**ing** anomalous activity to a high level of confidence by (a) logging network traffic **(b**) maintaining logs and other data collected **on** network traffic, **and (c) includes processes that are capable of protecting** evidence from compromised devices**. so that mitigations can be developed to improve responsible entity security against future similar attacks.**

3. Section addressing related Standards or SARs:

i. EEI agrees that close coordination will be needed between the Project 2016-02 SDT and this SDT.

ii. Project 2019-03 should be struck from the list of Projects this SDT will need to coordinate. This project is no longer an active project.

iii EEI agrees the SDT should assess for any impacts to CIP-005 and CIP-010, largely due to possible impacts related to changes in definitions. However, we also believe that CIP-007 should also be included for the reasons identified in our comments.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

Evergy supoprts and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #1.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

AES Clean Energy supports MRO NSRF's comments on this Unofficial Comment Form - see below.

"The MRO NSRF suggests the detailed description section be modified with additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text:

'First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment.'

The use of the term 'baseline' could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable

Connectivity. The MRO NSRF suggests the following wording:

'First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model.'

The detailed description provides a list of required detections:

'Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment.'

The MRO NSRF requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010.

The following text is suggested:

'Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use.'

The detailed description also contains the following scoping requirement:

'And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by…'

The MRO NSRF suggests that the term 'to a high level of confidence' be removed. In a zero-defect compliance environment, the requirement to prove a high level of confidence is difficult as it is a subjective statement.

The MRO NSRF suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid duplicating requirements. It is unclear why CIP-013 is included in the SAR, the MRO NSRF asks for additional clarity in the SAR, if in fact CIP-013 is to remain in the SAR scope.

Likes 0	
Dislikes 0	

Response

Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI and the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Brandon Smith - APS - Arizona Public Service Co. - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	

AZPS agrees with the intended scope of the SAR, however also agrees with EEI's suggested changes to the "Detailed Description Section" as identified below:

a. Detail Description Section: Create new or modified **existing** CIP Reliability Standards that are **risk**-based and address the need for responsible entities to **utilize security processes, systems and tools that 1)** develop baselines of network traffic inside **an Electronic Security Perimeter; 2)** monitor **for** and detect unauthorized activity, connections, devices, and software inside **an Electronic Security Perimeter; 3) are capable of** identify**ing** anomalous activity to a high level of confidence by (a) logging network traffic **(b**) maintaining logs and other data collected **on** network traffic, **and (c) includes processes that are capable of protecting** evidence from compromised devices**. so that mitigations can be developed to improve responsible entity security against future similar attacks.**

These recommended changes simplify the scope language and align with existing NERC Reliability Standards.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group appreciated the opportunity to comment and is in general support of EEI's prepared comments with the following suggested modifications:

The use of the term "baseline", in the Detailed Description Section (item #1), could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. Additionally, the use of the term "baseline" could misalign with the term as used in other Standards like CIP-010.

WEC Energy Group further suggests the following modification based on EEI's prepared comments:
"Create new or modified CIP Reliability Standards that are risk-based and utilize security processes, systems and tools that 1) analyze network traffic inside an Electronic Security Perimeter. Require anomaly-based analysis, where a model of normal network traffic is created and potential malicious traffic is identified based on this model."

Likes 0	

Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	No
Document Name	
Comment	
NextEra Energy supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) does not agree with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric (SIGE) does not agree with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Lori Frisk - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed scope as described in the SAR, given that proposed modifications are limited to high impact BES Cyber Systems and medium impact BES Cyber Systems with ERC. Should low impact BES Cyber Systems be included at any point, AEP would have concerns regarding the cost and support required.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
It is recommended to perform the feasibility study to ensure there is adverse impact to the BES reliable operations prior to creating or revising the standards. Also, the project scope should include all ESPs, including the Medium Impact BES Cyber Systems without ERC that are connected in a network.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Request clarification on this Scope's language which says *The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.* Does this mean this project's scope may change based on the completed feasibility study? Request clarification on "implementing measures" in part (3) in the Detailed Description, which is different than "monitoring" in parts (1) and (2) "*(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.*" We believe this language mandates retaining evidence (saving logs). Request clarification of "insider threat" in Industry Need - "*Current CIP Reliability Standards are insufficient to protect against insider threats*" Insider threat could be another CIP Standard or another entity program. We believe this "insider threat" is within the monitored network. The term 'quicker mitigation' should refer to a metric, such as time lapse.	
Likes 0	
Dislikes 0	

Response	
Alison MacKellar - Constellation - 5,6	
Answer	Yes
Document Name	
Comment	
Constellation aligns with Exelon's comments. Alison Mackellar on behalf of Constellation Segments 5 and 6.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF membership agrees with the proposed scope of the SAR as it relates to FERC Order 887. The NAGF recommends that the concept under the Detailed Description, “(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices” be further aligned with the networking security controls intention versus device level security controls.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Request clarification on this Scope’s language which says "*The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.".* Does this mean this project’s scope may change based on the completed feasibility study? Request clarification on “implementing measures” in part (3) in the Detailed Description, which is different than “monitoring” in parts (1) and (2): “*(3)*	

implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices." We believe this language mandates retaining evidence (saving logs).

Request clarification of "insider threat" in Industry Need - "*Current CIP Reliability Standards are insufficient to protect against insider threats*"

Insider threat could be another CIP Standard or another entity program. We believe this "insider threat" is within the monitored network.

The term 'quicker mitigation' should refer to a metric, such as time lapse.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	Yes
Document Name	

Comment

Ameren agrees that the proposed measures are beneficial to the protection of the BES. However, Ameren believes that a phased approach, with the initial focus being on High Impact BES Cyber Systems, would benefit the implementation of INSM technology. High Impact BES Cyber systems are typically centrally located in or near a datacenter and benefit from economies of scale and speed of implementation; whereas, Medium Impact BES Cyber Systems require procurement of hardware, have more complex/niche and interconnected equipment, and are geographically dispersed with a higher volume of site locations, which will require additional time considerations for implementation.

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 with the proposed scope in terms of high impact and medium impact BES Cyber Systems with ERC. However, we do offer the following comments detailed in Question 2 for consideration.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed scope as described in the SAR, as the language is directly from FERC Order 887.	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
MidAmerican agrees with the Project Scope while supporting MRO NSRF and EEI comments regarding the Detailed Description.	
Likes 0	
Dislikes 0	
Response	
Jesus Calderon-Acevedo - Orlando Utilities Commission - 1 - SERC	
Answer	Yes
Document Name	
Comment	
As currently proposed, OUC believes the SAR drafting team should provide more information which addresses concerns regarding the proposed items that are being directed by FERC. When considering the drafting of the requirements as they relate to the creation and monitoring of a network baseline, the drafting team should clearly define what items are to be a part of the baseline along with how often baselines should be monitored and updated. Details regarding actionable items on baseline deviations need to also be clearly stated. There are concerns with whether or not the idea is to achieve 0% packet loss which would be unfeasible, as opposed to collecting a representative sample of network traffic. Additionally, there need to be clear regulations on outage periods for network monitoring to ensure that entities can conduct necessary maintenance and testing on the assets responsible for performing these functions without concern for falling into a state of non-compliance due to a temporary outage, whether it be scheduled or un-scheduled. The expectations regarding the amount of network traffic being captured and requirements on allowances for outages in monitoring (for testing/maintenance) must also be clearly defined. Considerations must also be had on the concerns regarding the monitoring of any real-time communications, as introducing this level of monitoring to systems that rely on low latency	

transmissions may see unintended impacts.

The SAR drafting team should ensure they consider the impacts on the classification of current non-CIP assets that are being used to monitor network traffic and the other requirements they may be beholden to should they need to be classified as CIP assets as this will have an increased impact on managing the OT environment and complying with additional standards such as CIP-004-7, CIP-007-6, CIP-010-4.

When drafting the requirements for the logging of network traffic, the drafting team needs to ensure reasonable limitations are put in place on the retention period of network logs due to the large amount of data that is generated by network traffic in order to avoid unnecessary burdens on entities when it comes to allocating storage for the purpose of maintaining these network logs.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2023-03 INSM SAR	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1,3,5,6, Group Name NIPSCO Compliance	
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	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	

Request clarification on this Scope's language which says

The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges, and potential solutions for those BES Cyber systems not in scope.

Does this mean this project's scope may change based on the completed feasibility study?

Request clarification on "implementing measures" in part (3) in the Detailed Description, which is different than "monitoring" in parts (1) and (2)

"*(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.*"

We believe this language mandates retaining evidence (saving logs).

Request clarification of “insider threat” in Industry Need -

“*Current CIP Reliability Standards are insufficient to protect against insider threats*”

Insider threat could be another CIP Standard or another entity program. We believe this “insider threat” is within the monitored network.

Likes 0	
Dislikes 0	

Response

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

Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	
Document Name	

Comment

MidAmerican agrees with the Project Scope while supporting MRO NSRF and EEI comments regarding the Detailed Description.

MidAmerican is concerned that a requirement to baseline network traffic may be inadvisably prescriptive, forestalling other potentially effective approaches. Also, a network traffic baseline would likely be a proprietary product of any INSM software, and not something that could be exported to satisfy evidencing requirements.

We are also concerned about the SAR directing a requirement to identify anomalous activity "to a high level of confidence." We don't see how a requirement could be drafted to a subjective level of performance and respectfully request removal of this phrase.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

Industry Need section

The phrase “to ensure the detection of anomalous network activity indicative of an attack in progress” is used. We suggest that this is a desirable goal,

but no technology or standard can 100% *ensure* this. As the next sentence in the SAR states, it may "increase the probability of early detection". We suggest removing/replacing the "to ensure" in this scoping document.

In that same section, we suggest rewording or removing broad statements like "Current CIP Reliability Standards are insufficient to protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds." As this INSM SAR is a scoping document for a standards development project and SDTs often refer to their SAR to answer scope questions, we suggest this clearly focus the team's scope to the specific issue at hand – detecting potential malicious activity on these networks that may have bypassed the ESP/EAP layer of defense. This scoping document should not state or imply the SDT's scope is to protect against all insider threats or address all aspects of supply chain vulnerabilities. As a team with a defined deadline, clear and concise scoping will be needed that supports the team in avoiding scope creep.

Purpose or Goal section

This section does not address how the proposed project provides the reliability-related benefit, as the heading indicates, but is instead an implementation scope statement. We would suggest that the purpose or goal of how INSM provides the reliability benefit will be of importance to the SDT as they work under a regulatory deadline on such a large and involved topic.

Related Standards or SARs section

We find that Project 2019-03 was completed at the end of 2020 and no longer exists. We suggest removal of that project from this section and in its place add the Project 2023-04 SAR which will be addressing "detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity" to insure coordination on these related topics. Project 2022-05 is also working on issues relating to "attempts to compromise" and some degree of coordination may be needed there. There are many concurrent CIP standard activities with impacts to each other.

We suggest close coordination with Project 2016-02 as it is also making forward-looking changes to CIP-005. Those changes affect this INSM project at least in these ways:

• 2016-02 is modifying the associated definitions (ESP/EAP/ERC) and Requirements to no longer prescribe the perimeter-based "castle/moat" network architecture only and enable Zero Trust-based architectures. That project is proposing removing all "internal/inside" and "external/outside" terminology and replacing it with "protected by" to better align with and allow for ZT architectures while remaining backward compatible. As this SAR and project have "internal network" in the name, coordination is necessary. Also, as the principle of ZT that no network is trusted comes to fruition and all network traffic is encrypted, this impacts the ability to monitor at the network layer. As the ZT principles also work to shrink the "ESP" down to an individual workload/container/device rather than a network, the concept of "internal" will need coordination with 2016-02 as it also works to make the CIP standards incorporate these forward-looking options.

• 2016-02 is also addressing what is known as the "SuperESP" issue to remove impediments to the capability of seamlessly moving executing virtual servers from one location to another (e.g., primary to backup data center). Therefore 2016-02 is adding encryption requirements for portions of an "internal network" when a single ESP extends between different locations (though not using terms like inside/internal). The INSM SDT will need to coordinate with those changes as well.

As to the individual CIP standards mentioned in the SAR's scope, we understand CIP-005's inclusion for INSM, however the tie to CIP-010 concerning configuration management of an individual system and CIP-013 for supply chain procurement processes is unclear. We suggest that a review of CIP-007 R4's "Security Event Monitoring" may need to be included (see discussion concerning Zero Trust above) as well as CIP-008 with its "attempts to

compromise” concepts and requirements.

It is for these reasons that we suggest INSM may become more host/hypervisor/policy engine based in the future rather than “on the wire” packets as networks incorporate more end-to-end encryption and that CIP-007 (and its R4 Security Event Monitoring) would have a more direct tie to this SAR and need to be included.

We suggest making note of these (at a high level) in the SAR so these overlapping issues with 2016-02, 2023-04, and 2022-05 are known and coordinated.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	

Comment

SPP supports the comments submitted by the SRC and MRO NSRF.

SPP would ask the SDT to consider the potential cost that may arise from the scope of this SAR. As noted in other supporting documents related to INSM the costs associated with capturing, analyzing and storing of all data between every cyber assets within an ESP, for any length of time, will be substantial. Not all network architectures are created equal and could be costly and time consuming to implement for some responsible entities than others. Virtualization of network, server and storage infrastructure and the complexity it brings to the table has the potential to make packet captures, baselining of traffic, monitoring, analyzing and alerting much more difficult if a responsible entity is unable to obtain visibility into all of the network traffic within a subnet.

Likes 0	

Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
AES Clean Energy supports MRO NSRF's comments on this Unofficial Comment Form - see below. "The MRO NSRF suggests that the title of the SAR be updated to 'Electronic Security Perimeter Internal Network Security Monitoring' to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC)."	
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 RSC	
Answer	
Document Name	
Comment	
Request consideration of cloud-based monitoring solutions.	
Likes 0	

Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments submitted by the ISO/RTO Council Standards Review Committee	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
Request consideration of cloud-based monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2023-03 INSM SAR	
Answer	
Document Name	
Comment	
The IRC SRC supports the forward-looking, objective-based approach in the SAR for addressing the three goals outlined in the SAR. The eventual drafting team will need to provide clear definitions of what constitutes a “baseline” to establish anomalous activity. Responsible entities will need that clarification in order to determine what changes are going to be required (if any) to establish and maintain compliance with the new or revised standard/s.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	
Comment	
NST suggests the Standard Drafting Team be tasked with considering whether internal network connections used for time-sensitive protection or control functions between intelligent electronic devices be exempted from new "INSM" requirements in order to avoid potential problems caused by INSM latency.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
Manitoba Hydro suggests that the title of the SAR be updated to “Electronic Security Perimeter Internal Network Security Monitoring” to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC).	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation aligns with Exelon's comments. Alison Mackellar on behalf of Constellation Segments 5 and 6.	
Likes 0	

Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SAR, however, some additional explanation may be needed as to what is changing, since the information is vague. For example, network traffic is already logged, logs can be used to support incident investigation, implementing measures for maintaining logs and other data can be used for comparison analysis in unlikely event of attacker trying to remove/cover up activity. In addition, what is to be done differently at our Control Centers? Currently, we are already doing what is being proposed, such as logging networking traffic, and maintaining logs and other network traffic data collected, sufficient to draw meaningful conclusions and support incident investigation. Plus, we maintain the integrity of those logs and other data.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
Request consideration of cloud-based monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
When drafting the Standard and implementation guidance, Tacoma Power recommends that the SDT consider entities who have implemented a zero trust environment. For these entities, the implementation of INSM is unneccassary because there is no trusted network that requires monitoring.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The MRO NSRF suggests that the title of the SAR be updated to “Electronic Security Perimeter Internal Network Security Monitoring” to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC).	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2023-03 Internal Network Security Monitoring (INSM) Standard Authorization Request Drafting Team

Do not use this form for submitting nominations. Use the electronic form to submit nominations for **Project 2023-03 Internal Network Security Monitoring** Standard Authorization Request (SAR) drafting team members by **8 p.m. Eastern, Friday, May 5, 2023.** 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, Laura Anderson (via email), or at 404-782-1870.

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.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for internal network security monitoring of all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic once it is within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements that are "forward-looking, objective-based"[2] and address three security objectives outlined in Order No. 887. FERC directed NERC to submit these revisions for approval by July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of a lack of INSM for medium impact BES Cyber Systems without ERC, all low impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC is conducting the study, which is to be filed with FERC by January 18, 2024.

Standard(s) affected: CIP-005-7, CIP-010-4, and CIP-013-2

Drafting Team activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings, and conference calls. Approximately one to two face-to-face meeting per quarter can be expected (on average three full working days each

[1] Internal Network Security Monitoring for High and Medium Impact Bulk electric System Cyber Systems, Order No. 887, 182 FERC ¶ 61,021 (Jan. 19, 2023).
[2] Order No. 87 at P 5.

meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the drafting team sets forth. NERC is seeking individuals who possess experience in the following areas:

- Experience with IT/OT Network Engineering
- Understanding of Security Information and Event Monitoring
- Understanding of Cyber Threat Hunting
- Experience with Cyber Security Management Controls
- Understanding of BES Cyber Asset Low Impact Criteria
- Understanding of reliability risks associated with BES Cyber Assets and BES Cyber Systems
- Understanding of coordinated attack risks and mitigation options
- Understanding of external routable connectivity (ERC)
- Understanding of authentication for remote users
- Understanding of protection of user authentication information
- Understanding of detection of malicious communications
- Responsible entity compliance related to the areas listed above

Name:	
Organization:	
Address:	
Telephone:	
Email:	
Please briefly describe your experience and qualifications to serve on the requested SAR 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):
Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.
☐ Yes, the nominee has read and understands these documents.

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[3] 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:	
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:	

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-03 Internal Network Security Monitoring (INSM)

Nomination Period Open through May 5, 2023

Now Available

Nominations are being sought for **Project 2023-03 Internal Network Security Monitoring** Standard Authorization Request (SAR) drafting team members through **8 p.m. Eastern, Friday, May 5, 2023.**

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 one to 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 drafting 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 team 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 SAR drafting team in May 2023. Nominees will be notified shortly after they have been appointed.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-446-9671. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

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:	Internal Network Security Monitoring (INSM) (as revised by the Standard Drafting Team)		
Date Submitted:	March 7, 2023 (August 23, 2023)		
SAR Requester			
Name:	Michaelson Buchanan, Dan Goodlett, Larry Collier (Revised by Project 2023-03 Standard Drafting Team)		
Organization:	NERC		
Telephone:	470.725.5268, 470.522.7367, 470.716.2923	Email:	Michaelson.buchanan@nerc.net Dan.goodlett@nerc.net Larry.Collier@nerc.net
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 the CIP Reliability Standards require monitoring of the Electronic Security Perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This represents a gap in the currently effective CIP Reliability Standards. To address this gap, CIP Reliability Standards should be created or modified to require INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack. Current CIP Reliability Standards are insufficient to protect			

Requested information
against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
As directed by FERC Order No. 887, modify or create new Standard(s) that require INSM within a trusted Critical Infrastructure Protection networked environment for all high impact BES Cyber Systems with and without ERC and medium impact BES Cyber Systems with ERC.
Project Scope (Define the parameters of the proposed project):
The Standards Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order[1]. The scope of the project will include: • All high impact BES Cyber Systems; and • All medium impact BES Cyber Systems with ERC. The scope of the project should not extend to: • medium Impact BES Cyber Systems without ERC; or • low impact BES cyber systems.
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[2] 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):
Create new or modified existing CIP Reliability Standards that are forward-looking, objective-based, and that address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communications, and software inside the CIP-networked environment. And third, any new or modified CIP Reliability Standards should provide flexibility to responsible entities in how they identify anomalous activity to a high level of confidence by: (1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs, and other data collected, regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.

[1] The SDT is aware that the ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber Systems not in scope.
[2] 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.

Requested information
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Beyond the time and resources needed to serve on the Standard Drafting Team, the cost to entities will vary based on their current system architecture. While many entities may have the controls in place, others may not which could require a significant cost investment depending on their footprint.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None.
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):
Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The SAR has been developed in response to FERC Order No. 887. The final Order was consistent with feedback provided by NERC and industry through the NOPR process. NERC and the ERO Enterprise have convened a response team to address directives in the FERC Order which included a review of this SAR.
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)?
The following projects and Reliability standards should be assessed for impact: • Projects 2016-02 and 2022-05 • Reliability Standards CIP-005, CIP-007, CIP-008, CIP-010, and CIP-013
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.
This Standards Authorization Request has been developed pursuant to FERC Order No. 887.

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] 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.

Reliability Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

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
N/A	

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
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

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:	Internal Network Security Monitoring (INSM) (as revised by the Standard Drafting Team)		
Date Submitted:	March 7, 2023 (August 23, 2023)		
SAR Requester			
Name:	Michaelson Buchanan, Dan Goodlett, Larry Collier (Revised by Project 2023-03 Standard Drafting Team)		
Organization:	NERC		
Telephone:	470.725.5268, 470.522.7367, 470.716.2923	Email:	Michaelson.buchanan@nerc.net Dan.goodlett@nerc.net Larry.Collier@nerc.net
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 the CIP Reliability Standards require monitoring of the Electronic Security Perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This ~~presents~~ represents a gap in the currently effective CIP Reliability Standards. To address this gap, CIP Reliability Standards should be created or modified to require INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack. Current CIP Reliability Standards are insufficient to			

Requested information
protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
As directed by FERC Order No. 887, modify or create new Standard(s) that require INSM within a trusted Critical Infrastructure Protection networked environment for all high impact BES Cyber Systems with and without ERC and medium impact BES Cyber Systems with ERC.
Project Scope (Define the parameters of the proposed project):
The Standards Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order[1]. The scope of the project will include: • All high impact BES Cyber Systems~~,~~ ; and • All medium impact BES Cyber Systems with ERC. The scope of the project should not extend to: • medium Impact BES Cyber Systems without ERC; or • low impact BES cyber systems. ~~The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.~~
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[2] 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):
Create new or modified existing CIP Reliability Standards that are forward-looking, objective-based, and that address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communications, and software inside the CIP-networked environment. And third, any new or modified CIP Reliability Standards should provide flexibility to ~~require~~ responsible entities ~~to~~ in how they identify anomalous activity to a high level of confidence by: (1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs, and other data collected, regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.

[1] The SDT is aware that the ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber Systems not in scope.

[2] 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.

Requested information
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Beyond the time and resources needed to serve on the Standard Drafting Team, the cost to entities will vary based on their current system architecture. While many entities may have the controls in place, others may not which could require a significant cost investment depending on their footprint.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None.
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):
Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, ~~Interchange Coordinator, Interchange Authority,~~ Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[3] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The SAR has been developed in response to FERC Order No. 887. The final Order was consistent with feedback provided by NERC and industry through the NOPR process. NERC and the ERO Enterprise have convened a response team to address directives in the FERC Order which included a review of this SAR.
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)?
The following projects and Reliability standards should be assessed for impact: • Projects 2016-02~~, 2019-03~~ and 2022-05 • Reliability Standards CIP-005~~-7~~, CIP-007, CIP-008, CIP-010~~-4~~, and CIP-013~~-2~~
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.
This Standards Authorization Request has been developed pursuant to FERC Order No. 887.

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] 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.

Reliability Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

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
N/A	

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
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Project 2023-03 Internal Network Security Monitoring

Action

- Accept the revised Project 2023-03 INSM Standard Authorization Request (SAR);
- Authorize drafting of Reliability Standard(s) identified in the SAR; and
- Approve a waiver of provisions of the Standard Processes Manual for Project 2023-03 Internal Network Security Monitoring (INSM) due to regulatory deadlines, as follows:
  - Initial formal comment and ballot period reduced from 45 days to as few as 30 calendar days, with ballot pools formed in the first 20 days, and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last 5 days of the comment period (Sections 4.9, 4.10);
  - Additional formal comment and ballot period(s) reduced from 45 days to as few as 20 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period (Sections 4.9, 4.10).
  - Final ballot reduced from 10 days to as few as five calendar days (Section 4.13)

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues. In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC is currently conducting the study, which is to be filed with FERC by January 18, 2024.

The Standards Committee (SC) accepted the SAR at its March 22, 2023 meeting. At that same meeting, the SC authorized soliciting members for the Standard Drafting Team (SDT). The formal comment period and the solicitation for the SDT member period ran from April 6 - May 5, 2023. The SC appointed the chair, vice chair, and members to the Project 2023-03 INSM SDT.

The SDT reviewed and considered all comments received by industry and revised the SAR where appropriate.

Due to the July 9, 2024 deadline, the SC is being asked to waive those portions of Sections 4.7, 4.9, and 4.13 as they relate to the minimum required length for comment periods and ballots, including the final ballot. Section 16.0 of the Standards Processes Manual provides:

The Standards Committee may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:

- In response to a national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber attack on the BES
- Where necessary to meet regulatory deadlines;
- Where necessary to meet deadlines imposed by the NERC Board of Trustees; or
- Where the Standards Committee determines that a modification to a proposed Reliability Standard or its Requirement(s), a modification to a defined term, a modification to an Interpretation, or a modification to a Variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

Summary

NERC staff recommends that the SC accept the revised SAR, authorize drafting revisions to the standards listed in the SAR, and issue a waiver of Sections 4.7, 4.9, and 4.13 as they relate to the minimum required length for comment periods and ballots in order to meet the regulatory deadline established by FERC.

Consistent with Chapter 7 of the SC Charter, if the schedule requires, NERC staff would seek authorization from the SC Executive Committee in a properly noticed and open session to post the Reliability Standard(s) developed through this project for the initial formal comment period and ballot. Depending on when the standard(s) is ready to post, this flexibility would allow as much time for development work and comment periods as possible before the July 2024 deadline.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minutes
Standards Committee Meeting

A. Casuscelli, chair, called to order the meeting of the Standards Committee (SC) on August 23, 2023, at 1:02 p.m. Eastern. A. Oswald called roll and determined the meeting had a quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement
The SC secretary called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice and directed questions to NERC's General Counsel, Sonia C. Rocha.

Introduction and Chair's Remarks
A. Casuscelli welcomed the SC, guests, and proxies to the meeting.

Review August 23, 2023 Agenda (agenda item 1)
The SC approved the August 23, 2023 meeting agenda.

Consent Agenda (agenda item 2)
The SC approved the July 19, 2023 SC Meeting Minutes. The SC was informed about Project 2023-04 Modifications to CIP-003 SC Action without a Meeting.

Projects Under Development (agenda item 3)
C. Yeung reviewed the Project Tracking Spreadsheet. L. Harkness reviewed the Project Posting Schedule.

Project Management Posting Coordination (agenda item 4)
M. Brytowski provided an overview of the Project Management Oversight Subcommittee (PMOS) posting coordination. C. Yeung provided insight into how liaisons could work with developers and drafting team (DT) leadership to coordinate schedules. S. Kim shared that Standard Development is looking to host a webinar that details the prioritization of projects and the risk registry update. Discussion will continue to the next SC meeting.

Legal Update and Upcoming Standards Filings (agenda item 9)
L. Perotti provided an update.

Errata to Reliability Standard TOP-003-6 (agenda item 6)
L. Harkness provided an overview of the errata changes. V. O'Leary motioned to accept the errata changes to TOP-003-6 to remove the word "using" from Requirement R5 and correct the grammar of the word "methods" in Requirement R2 Part 2.5.5.

The SC approved the motion with no objections or abstentions.

Project 2023-03 Internal Network Security Monitoring (agenda item 5)
J. Calderon provided an overview of the project background and standard authorization request (SAR). S. Rueckert made a motion to accept the revised Project 2023-03 Internal Network Security Monitoring Standard Authorization Request (SAR), authorize drafting of Reliability Standard(s) identified in the SAR, and approve a waiver of provisions of the Standard Processes Manual for Project 2023-03 Internal Network Security Monitoring (INSM) due to regulatory deadlines, as follows:

- Initial formal comment and ballot period reduced from 45 days to as few as 30 calendar days, with ballot pools formed in the first 20 days and initial ballot and non-binding poll of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) conducted during the last five days of the comment period (Sections 4.9, 4.10);
- Additional formal comment and ballot period(s) reduced from 45 days to as few as 20 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period (Sections 4.9, 4.10).
- Final ballot reduced from 10 days to as few as five calendar days (Section 4.13)

The SC approved the motion with no objections or abstentions.

Project 2021-08 Modifications to FAC-008 (agenda item 7)
J. Calderon provided an overview of the project background. V. O'Leary asked if the additional requirement nine aligned with the SAR's scope. B. Wu shared that requirement nine complements requirement 6, which requirement 9 focuses on maintaining data to keep requirement six enforceable. V. O'Leary made a motion to authorize initial posting of the proposed Reliability Standard FAC-008-6 and the associated Implementation Plan for a 45-day formal comment period, with ballot pools formed in the first 30 days and parallel initial ballots and non-binding polls on the VRFs and VSLs, conducted during the last 10 days of the comment period.

The SC approved the motion with no objections or abstentions.

Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination (agenda item 8)
L. Harkness provided an overview of the project's background. S. Rueckert inquired when the SDT would have to respond to comments from the last formal comment period. A. Oswald mentioned that the SDT would have enough time to respond to comments. S. Rueckert made a motion to approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2021-07:

- Additional formal comment and ballot period (s) reduced from 45 days to as little as 20 days, with the ballot conducted during the last 10 days of the comment period. (Sections 4.9 and 4.12)
- Final ballot reduced from 10 days to five calendar days. (Section 4.9)

The SC approved the motion with no abstentions. William Chambliss, Kent Feliks, and Terri Pyle opposed.

R. Blohm asked about the classifications of NERC membership sectors and, specifically, inquired about the ”associate” category and how it is defined. L. Perotti explained how the NERC membership sectors differ from the registered body segments and provided a brief overview.

Adjournment

The meeting adjourned at 2:29 p.m. Eastern.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Committee
2023 Segment Representatives

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Chair 2022-23	Amy Casuscelli* Manager, Reliability Assurance & Risk Management	Xcel Energy		X
Vice Chair 2022-23	Todd Bennett* Managing Director, Reliability Compliance & Audit Services	Associated Electric Cooperative, Inc.		X
Segment 1-2022-23	Michael Jones Manager, Reliability Standards & Policy	National Grid		X
Segment 1-2021-22	Troy Brumfield* Regulatory Compliance Manager	American Transmission Company		X
Segment 2-2022-23	Jamie Johnson Infrastructure Compliance Manager	California ISO		N
Segment 2-2021-22	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool		X
Segment 3-2022-23	Kent Feliks Manager NERC Reliability Assurance – Strategic Initiatives	American Electric Power Company, Inc.		X
Segment 3-2021-22	Vicki O' Leary Director – Reliability, Compliance, and Implementation	Eversource Energy		X
Segment 4-2022-23	Marty Hostler Reliability Compliance Manager	Northern California Power Agency		X
Segment 4-2021-22	Patti Metro Senior Grid Operations & Reliability Director	National Rural Electric Cooperative Associate	Alice Wright	X
Segment 5-2022-23	Terri Pyle Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric		X
Segment 5-2021-22	Jim Howell Markets Compliance Manager	Southern Company Generation		X

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Segment 6-2022-23	Sarah Snow* Manager of Reliability Compliance	Cooperative Energy		X
Segment 6-2021-22	Justin Welty Senior Manager, NERC Reliability Standards	NextEra Energy		X
Segment 7-2022-23	Kristine Martz Industry Specialist, Power & Utilities	Amazon Web Services		X
Segment 7-2021-22	Venona Greaff* Senior Energy Analyst	Occidental Chemical Corporation		X
Segment 8-2022-23	Robert Blohm[1] Managing Director	Keen Resources Ltd.		X
Segment 8-2021-22	Philip Winston Retired (Southern Company)	Independent		X
Segment 9-2022-23	Sarosh Muncherji[1] Cyber Security Specialist	British Columbia Utilities Commission		X
Segment 9-2021-22	William Chambliss General Counsel	Virginia State Corporation Commission		X
Segment 10-2022-23	Tony Purgar Senior Manager, Operational Analysis & Awareness	ReliabilityFirst		X
Segment 10-2021-22	Steven Rueckert Director of Standards	WECC		X

[1] Serving as Canadian Representative
*Denotes SC Executive Committee Member

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023

Anticipated Actions	Date
35-day formal comment period with ballot	12/14/2023 – 1/17/2024
XX-day formal comment period with additional ballot	TBD
XX-day final ballot	TBD
Board adoption	TBD

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 – System Security Management

2. **Number:** CIP-007-X

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural 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 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 Special Protection System (SPS) where the SPS 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-007-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-002-5.1 identification and categorization processes.

5. Effective Date: See Implementation Plan for CIP-007-X.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R2 – Security Patch Management*. *[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-007-X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R2 – Security Patch Management			
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	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-X Table R2 – Security Patch Management			
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	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R3 – Malicious Code Prevention			
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	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	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	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	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	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – Internal Network Security Monitoring (INSM)* to increase the probability of detecting an attack that has bypassed other security controls. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment].*

M6. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – INSM* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.	Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

CIP-007-X Table R6 – INSM			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary.

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 Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R1. (R1)
R2.	The Responsible entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	included the applicable items in CIP-007-X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	or revised within the timeframe specified in the plan. (2.4)
R3.	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)
R4.	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more	process(es) that included the applicable items in CIP-007-X Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	
R5.	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts.	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access, but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar	process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			months of the last password change. (5.6)	obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)
R6.	The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).	The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).	The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3). OR The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices,	The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6). OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			and network communications using data from Part 6.2 (6.4). OR The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).	The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1). OR The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).

C. Regional Variances

None.

D. 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	Approved 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-007-5.	
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	2/15/15	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-007-X. Docket No. RM15-14-000	
X	06/2023	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on xx/xx/xx. Revised version addresses Order No. 887 related to Internal Network Security Monitoring.

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023

Anticipated Actions	Date
35-day formal comment period with ballot	12/14/2023 – 1/17/2023
XX-day formal comment period with additional ballot	TBD
XX-day final ballot	TBD
Board adoption	TBD

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 – System Security Management

2. **Number:** CIP-007-~~6~~X

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~3.~~4. **Applicability:**

~~3.1.~~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.

~~3.1.1~~4.1.1 **Balancing Authority**

~~3.1.2~~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:

~~3.1.2.1~~4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

~~3.1.2.1.1~~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

~~3.1.2.1.2~~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.

~~3.1.2.2~~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.

~~3.1.2.3~~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.

~~3.1.2.4~~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.

~~3.1.3~~4.1.3 **Generator Operator**

~~3.1.4~~4.1.4 **Generator Owner**

~~3.1.5~~4.1.5 **Interchange Coordinator or Interchange Authority**

~~3.1.6~~4.1.6 **Reliability Coordinator**

~~3.1.7~~4.1.7 **Transmission Operator**

~~3.1.8~~4.1.8 **Transmission Owner**

~~3.2.~~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.

~~3.2.1~~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:

~~3.2.1.1~~4.2.1.1 Each UFLS or UVLS System that:

~~3.2.1.1.1~~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

~~3.2.1.1.2~~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.

~~3.2.1.2~~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.

~~3.2.1.3~~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.

~~3.2.1.4~~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.

~~3.2.2~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

~~3.2.3~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-X:

~~3.2.3.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~3.2.3.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~3.2.3.3~~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.

~~3.2.3.4~~4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~3.2.3.5~~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.

~~4.~~5. **Effective Date:** See Implementation Plan for CIP-007-~~6~~X.

~~5. **Background:** Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires 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-002-5.1 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 at Control Centers –** Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**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 in the applicability column. 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.~~

- ~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X~~6~~ Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X~~6~~ Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~6~~ X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

~~M1.~~M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
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	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
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	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~6~~ X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES -Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

~~M2.~~M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
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	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~6~~ X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	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	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-~~6~~ X Table R3 – ~~-~~Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

~~M3.~~M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~ X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

~~M4.~~M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	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	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~6~~ XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, ~~-~~the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~ X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – Internal Network Security Monitoring (INSM)* to increase the probability of detecting an attack that has bypassed other security controls. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment].*

M6. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – INSM* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods

6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

6.4	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.

6.5	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.	Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.

6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary. ~~b R6, Part~~

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 Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R1. (R1)
R2.	The Responsible entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	included the applicable items in CIP-007-~~6~~ X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	or revised within the timeframe specified in the plan. (2.4)
R3.	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)
R4.	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more	process(es) that included the applicable items in CIP-007-~~6~~ X Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	
R5.	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~ X Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) ~~OR~~ ~~The Responsible Entity has implemented one or more~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5)~~	~~documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)~~ OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R6.	The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).	The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).	The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3). OR The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2 (6.4). OR The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).	The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6). OR The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).

C. Regional Variances

None.

D. 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	Approved 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-007-5.	
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	2/15/15	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-007-~~6~~X. Docket No. RM15-14-000	
X	06/2023	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on xx/xx/xx. Revised version addresses Order No. 887 related to Internal Network Security Monitoring.

~~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:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device-level requirement. If a device has no provision for disabling or restricting logical ports on the device (example – purpose-built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

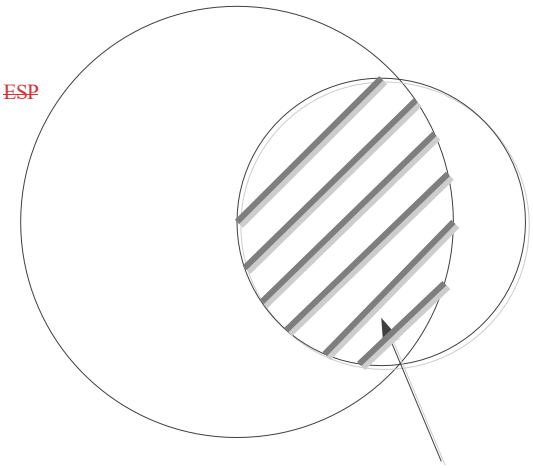
This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense in depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components

PSP

ESP



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an

"install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock

~~starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the~~

~~Cyber Asset's baseline.~~

~~Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the~~

~~Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch~~

~~Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.1.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can~~

~~document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.2. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~Requirement R4:~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.2.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer-generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.3.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~Detected known or potential malware or malicious activity~~
- ~~Failure of security event logging mechanisms~~
- ~~Login failures for critical accounts~~
- ~~Interactive login of system accounts~~
- ~~Enabling of accounts~~
- ~~Newly provisioned accounts~~
- ~~System administration or change tasks by an unauthorized user~~
- ~~Authentication attempts on certain accounts during non-business hours~~
- ~~Unauthorized configuration changes~~
- ~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~Requirement R5:~~

~~Account types referenced in this guidance typically include:~~

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~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 requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-007-X

Applicable Standard(s)

- CIP-007-X – Cyber Security – System Security Management

Requested Retirement(s)

- CIP-007-7 – Cyber Security – System Security Management[1]

Applicable Entities

- Balancing Authority
- Distribution Provider[2]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues. In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and

[1] If CIP-007-7 is not in effect, the currently effective version would be retired.

[2] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

solutions for implementing INSM for those BES Cyber Systems. NERC is currently conducting the study, which is to be filed with FERC by January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement new Requirement R6. In order to achieve the objectives of Requirement R6, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with the new requirements specific to Reliability Standard CIP-007-X, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-007-X Cyber Security – System Security Management

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) 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 thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-007-X Cyber Security – System Security Management - Requirement R6

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1 and R1.2 shall initially comply with the requirements in CIP-007-X Requirement R6 for those Control Centers upon the effective date of Reliability Standard CIP-007-X. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-007-X Requirement R6 within 24 calendar months after the effective date of Reliability Standard CIP-007-X. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.

Retirement Date

Reliability Standard – CIP-007-7 Cyber Security – System Security Management

Reliability Standard CIP-007-7[3] shall be retired immediately prior to the effective date of Reliability Standard CIP-007-X in the particular jurisdiction in which the revised standard is becoming effective.

[3] If CIP-007-7 is not in effect, the currently effective version would be retired.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-03 Internal Network Security Monitoring

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2023-03 INSM/CIP-007-X Cyber Security – Systems Security Management** by **8 p.m. Eastern, Wednesday, January 17, 2024.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Laura Anderson, or at 404-782-1870.

Background Information

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for Internal Network Security Monitoring (INSM) of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard requirements for any new or modified CIP Reliability Standards that address three security issues.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats and incidents. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

The Project 2023-03 Standard Drafting Team (SDT) Draft 1 of proposed CIP-007-X requires responsible entities to implement an NSM system. Responsible entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks.

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 provides that any new or modified CIP Reliability Standards should address (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; ad (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *See id.* P 5.

INSM refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the trusted CIP related operational zones of the responsible entity, and also includes select associated systems such as: Physical Access Control Systems (PACS) and Electronics Access Control Systems (EACMS).

Order No. 887 included the phrase "CIP-Networked Environment." INSM monitoring should include communications between EACMS (e.g., Active Directory, 2FA, or RADIUS) and PACS. Order No. 887 specifically excluded some components of a "CIP-Networked environment;" including low impact BES Cyber Systems (BCS) and medium impact BCS without ERC. The exclusion was narrow and limited, but did not exclude EACMS or PACS devices.

The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) shall be inclusive of the following:

- ESP(s) associated with high impact BCS and their associated PCAs
- Routable communications between EACMS (either internal or external to the ESP) associated with high impact BCS
- Routable communications between EACMS and PACS associated with high impact BCS
- ESP(s) associated with medium impact BCS with External Routable Connectivity and their associated Protected Cyber Assets (PCAs)
- Routable communications between EACMS (either internal or external to the ESP) associated with medium impact BCS with ERC
- Routable communications between EACMS and PACS associated with medium impact BCS with ERC

CIP-networked environment is inclusive of CIP devices (BCS, EACMS, PACS, and PCAs) only and does not require the monitoring of network data containing devices outside the scope CIP.

CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device (including other PACS devices) is out of scope.

The SDT considered several options regarding the addition of INSM requirements to the CIP framework: including the addition of INSM by revising an existing standard, or addition of an entirely new standard. To inform this decision, the SDT primarily considered Order No. 887, schedule expectations, and the fundamental principles of NSM.

The SDT concluded that INSM requirements would best align as revisions to CIP-007 since the outcomes of INSM most closely align with management of security systems, particularly regarding collection and analysis of system data. INSM is a distinct function independent of the logging requirements already established in CIP-007, but taken together, INSM and the currently approved CIP-007 requirements will complement each other in helping responsible entities improve overall management of security systems.

An alternative was identified to optionally revise CIP-005 to include INSM requirements or create a new standard. This secondary option was declined due to the focus of CIP-005 on establishing and maintaining secure CIP network perimeters, which is essentially a different outcome than the intention of INSM. The SDT felt that creating a new Reliability Standard would not be necessary, but is open to feedback.

The SDT expects significant discussion about the Applicable Systems section of the proposed Requirement R6 parts of CIP-007-X; specifically, conditional inclusion of EACMS, PACS, and PCA devices. INSM can be a very powerful tool for defense teams protecting critical functions, though it does have limitations. Understanding these strengths and weaknesses in context of the networks supporting BES Cyber Assets produced the proposed "Applicable Systems" section.

This Draft 1 proposed CIP-007-X applies to CIP networks that contain high impact BCS and medium impact BCS environments that also have ERC consistent with Order No. 887. Associated PCA are also contained in the ESP that contain high impact BES BCS and medium impact BCS that have ERC. The Draft 1 proposed that CIP-007-X applies to PACS and EACMS in two main ways: first, if those PACS or EACMS are contained within or on the ESP of a high or qualifying medium Impact CIP environments; and second if the network communications are between a PACS and an EACMS associated with a high or qualifying medium impact CIP environment.

INSM is primarily focused on internal network communications within these protected environments, and that includes communication that has traversed the Electronic Access Point (EAP). INSM also applies to EACMS and PACS related to, but outside of, qualifying CIP high and medium environments due to the possibility of a threat actor's need to manipulate such external systems in order to gain access to the protected CIP environments.

The intention of the SDT is not that all communications outside of the ESP be included in INSM, particularly the encrypted traffic that has exited a protected zone, or the entirety of an enterprise's business networks.

Order No. 887 included the phrase "CIP-Networked Environment." INSM monitoring should include communications between electronic access control systems (e.g., Active Directory, two-factor authentication, or RADIUS) and PACS. Order No. 887 specifically excluded some components of a "CIP-Networked environment;" including low impact BCS and medium impact BCS without ERC. The exclusion was narrow and limited, but did not exclude EACMS or PACS devices.

Questions

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

   ☐ Yes
   ☐ No

   Comments:

3. Order No. 887 also references "CIP-Network Environment" that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. The Project 2023-03 SDT held extensive conversations about the term "baseline" and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT's use of the term "network communications 'baseline'" is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term "anomalous." The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of "anomalous" was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term "anomalous" was the appropriate term to use to describe that methodology. Do you agree that that the term "anomalous" effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

    ☐ Yes
    ☐ No

    Comments:

11. Please provide any additional comments for the SDT to consider, if desired.

    Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

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 2023-03 INSM. 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-007, Requirement R1

The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VSL Justification for CIP-007, Requirement R1

The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VRF Justification for CIP-007, Requirement R2

The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VSL Justification for CIP-007, Requirement R2

The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VRF Justification for CIP-007, Requirement R3

The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VSL Justification for CIP-007, Requirement R3

The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VRF Justification for CIP-007, Requirement R4

The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VSL Justification for CIP-007, Requirement R4

The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VRF Justification for CIP-007, Requirement R5

The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VSL Justification for CIP-007, Requirement R5

The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard

VRF Justifications for CIP-007-X, Requirement R6	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) to increase the probability of detecting an attack that has bypassed other security controls. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es), the VRF is reflective of the implementation as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R6 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium for Requirement R6 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-007-X, Requirement R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).	The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).	The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3). OR The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2 (6.4). OR The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).	The Responsible Entity did not ~~i~~include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6). OR The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1). OR The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).

VSL Justifications for CIP-007-X, Requirement R6	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-007-X

CIP-007-X – Cyber Security – System Security Management

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-X. It also provides guidance to responsible entities for clarifying Internal Network Security Monitoring (INSM) systems and the original intent of the Standard Drafting Team (SDT). This Technical Rationale document for CIP-007-X is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats and incidents. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

The Project 2023-03 SDT proposed Reliability Standard CIP-007-X requires responsible entities to implement an NSM system. Responsible Entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks.

---

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following security issues: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

Responsible Entities are to evaluate their networks and identify the collection locations and methods most effective for their network configurations. Responsible entities will monitor and respond to anomalous communications and escalate these occurrences, if appropriate. Responsible entities will also appropriately protect NSM systems and data. In order to assist other entities and improve the nationwide security of electric systems, responsible entities are encouraged to share NSM data with technical and security support groups and peers: including law enforcement; defense organizations, such as the CISA; and industry partners and vendors. NSM will be an on-going, or possibly an iterative, process enabling responsible entities to actively identify, mitigate, and escalate threatening actions before they are allowed to impact the reliable operation of the BES.

INSM [i-en-es-em] is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the operational zones of the entity, and also includes associated systems; such as Physical Access Control Systems (PACS), access monitoring systems, and Electronics Access Control Systems (EACMS). While the entities are encouraged to use NSM systems at other critical networks, such as corporate internet perimeters, these requirements apply only to the applicable systems listed in the standard.

General Considerations

Regulatory changes to CIP-007, CIP-005, or a new standard

The SDT considered several options regarding the addition of INSM requirements to the CIP framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887[3], schedule expectations, and the fundamental principles of NSM as detailed in several books, such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4]; and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

The SDT concluded that INSM requirements would best align as an addition to Reliability Standard CIP-007 since the outcomes of INSM most closely align with management of security systems, particularly regarding collection and analysis of system data. INSM is a distinct function independent of the logging requirements already established in Reliability Standard CIP-007; but taken together, INSM and the pre-existing Reliability Standard CIP-007 requirements complement each other in helping responsible entities improve overall management of security systems.

System Classification

INSM systems will not carry a specific CIP term; such as Electronic Access Point (EAP) or EACMS. INSM systems, and some INSM components, may be classified as BES Cyber Systems Information Repositories (BCSI) or EACMS. INSM systems are commonly classified as BCS Information Repositories, which is an acceptable designation.

[3] *Id.*
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

An entity may choose to classify a standalone INSM system as an EACMS, but the entity should be aware that an INSM system using only network traffic cannot precisely determine if an encrypted login attempt is failed or successful (example encrypted protocols include ssh, https, RADIUS, and RDP). INSM systems may attempt to infer login success or failure using network data, such as session duration and amount of data transferred. Because of this limitation, INSM systems are a poor choice for monitoring and alerting on successful and failed electronic access when using encrypted protocols. Detection of events, such as failed and successful logons, is more precise when supplemented with endpoint logs.

Classification Rationale

INSM systems, as well as the networks they are monitoring, can be configured in a very wide array of possibilities. As such, the system classifications could also vary depending on the design implemented by the responsible entity. Ideally, INSM systems are segmented from the network components being monitored, as well as from the enterprise business network. Network communications very often also do not obviously contain physical location details for the assets joined to the network, but having this information readily available in the NSM system will make the system much more usable for the responsible entity. NSM system input data is most often duplicated network communication streams, copied through the use of a dedicated device, like a network tap, or through use of network switch port mirroring. Other options exist as well, such as using an endpoint device to collect and transfer duplicated network communication. All of these methods require transferring duplicated traffic to the NSM system via non-routable protocols, such as those sourced from a network tap or mirrored port, or it involves the transfer of duplicated data through the use of a routable protocol from an end device serving as a collector or monitoring sensor.

This traffic can all be securely sent outside of the primary CIP-networked environments being monitored. Ideally, the NSM system would only be designated as a BCSI; although portions, such as end point collectors, could be classified as Protected Cyber Assets (PCAs). Similarly, the responsible entities could designate INSM systems as an EACMS, however the intent of the SDT is that NSM focuses primarily on the collection, analysis, and response to abnormal network traffic. Collection of BCS alerts, logging, and authentication is best handled elsewhere.

Responsible entities are intended to leverage EACMS data, as well as any other pertinent information, to help provide context during analysis of network anomalies identified through INSM. Addition of INSM is not intended to replace or detract from the functions and requirements applied to EACMS.

INSM

The goal of INSM is to detect adversarial activity. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as Endpoint Detection and Response (EDR). By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While an entity may choose to implement active prevention measures in an INSM system, prevention is not expected in this requirement.

The principles of INSM as defined in Richard Bejtlich's book, *The Practice of Network Security Monitoring*, can be summarized in three main actions: collect, analyze, and escalate. The outcome of INSM is to establish an independent collection and monitoring system enabling cyber defenders to identify and respond appropriately to network activity caused by threat actors in preparation of an attack. Threat actors commonly take steps to hide their actions, and very often need to work for an extended period within targeted environments to develop disruption capabilities.

During successful cyber-attacks, these preparatory actions often go unnoticed. NSM Monitoring establishes capabilities to detect these actions independent of all the other security controls that are already in place. This enables defenders to take corrective actions to prevent and disrupt attacks prior to disruption. To be effective, NSM needs to maintain independence of monitored systems to avoid common modes of failure.

Vendor Support

The SDT is aware that some control system vendors have historically stated that their systems do not support cybersecurity monitoring using either INSM data collection or endpoint logging collection. The INSM collection requirements do not include the statement “per system capability” specifically because it is the intent of the SDT that every control system should have the capability to provide an appropriate level of visibility.

Requirement R6, Part 6.1 allows wide latitude to design supported cybersecurity data collection systems and allows vendors the option to gather cybersecurity information at the network and endpoint. Many control systems generate logs with relevant cybersecurity information, such as asset configuration, version levels, and access logs. A vendor-supported logging system may include forwarding existing logs to a cybersecurity monitoring tool, which could augment the INSM collection system.

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Information Sharing

A mature security monitoring program requires sharing of information with partners; including government, utility, and industry stakeholders. No part of these requirements should be interpreted to limit or restrict responsible entities from continuing maturity of their information sharing programs. Data components that are collected by INSM systems may be shared with government, industry, and utility partners and vendors. Specifically allowed for sharing are packet capture files, network traces, and other network metadata including internal IP addresses that could benefit other Registered Entities and partners. When sharing information, responsible entities may redact unnecessary components from shared data, such as SNMP community strings and unencrypted logins.

Entities are encouraged to participate with mature information sharing programs and partnerships.

Rationale for the Applicable Systems Section for Requirement R6 Parts

Summary

NSM can be a very powerful tool for defense teams protecting critical functions, though it does have limitations. Understanding these strengths and weaknesses in context of the networks supporting BCS produced the "Applicable Systems" of the Requirement R6 parts.

Draft 1 of proposed CIP-007-X applies to high impact BCS and medium impact BCS environments that also have ERC. Isolated medium impact environments, or medium impact environments that only utilize serial communications, are exempt. Associated PCAs in high and qualifying medium impact environments are also included.

Draft 1 of proposed CIP-007-X applies to PACS and EACMS that are contained within or on the perimeter of a CIP high or qualifying medium impact environment. CIP-007-X also applies to network communications between EACMS and PACS that is applicable to assets inside of qualifying CIP high or medium impact environments.

INSM is primarily focused on internal network communications within these protected environments, and that includes communication that has traversed the EAP. INSM also applies to EACMS and PACS related to, but outside of, qualifying CIP high and medium environments due to the possibility of a threat actor need to manipulate such external systems in order to gain access to the protected environments.

The intention of the SDT is not that all communications outside of the qualifying environments be included in INSM; particularly, the encrypted traffic that has exited a protected zone, or the entirety of enterprise business networks. The diagram below helps illustrate this intent.

CIP-networked environment

The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) shall be inclusive of the following (adjusted for clarity for the purposes of showing SDT development of revisions to CIP-007-X):

- ESP(s) associated with High Impact BES Cyber Systems and their associated PCAs
- Routable communications between EACMS (either internal or external to the ESP) associated with High Impact BES Cyber Systems
- Routable communications between EACMS and PACS associated with High Impact BES Cyber Systems
- ESP(s) associated with Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCAs
- Routable communications between EACMS (either internal or external to the ESP) associated with Medium Impact BES Cyber Systems with External Routable Connectivity
- Routable communications between EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity

CIP-networked environment is inclusive of CIP devices (BCS, EACMS, PACS and PCAs) only.
CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device is out of scope.

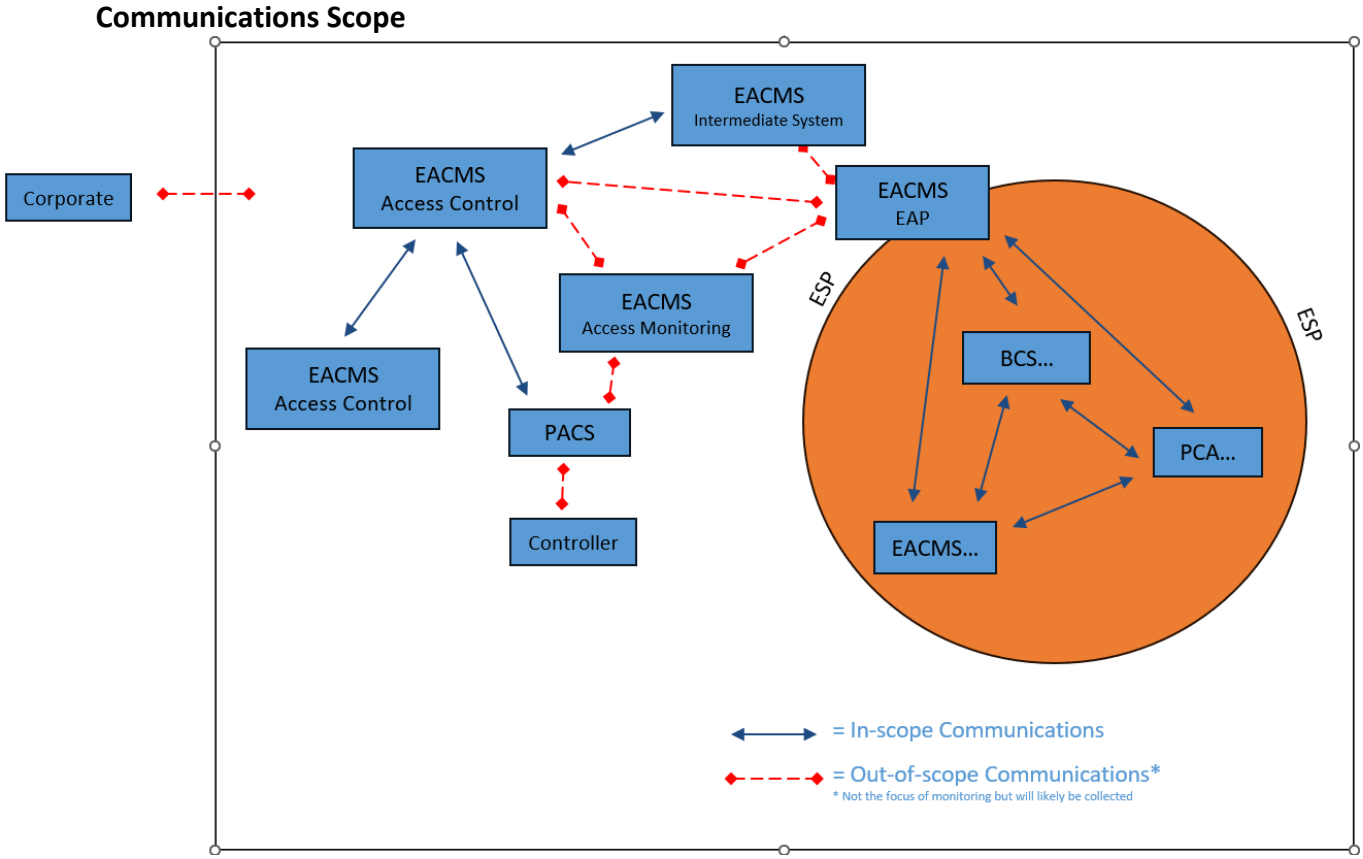


Figure 1

The SDT included these communications within the scope of the INSM Requirement R6 applicable systems.

Rationale for INSM Monitoring of associated EACMS, PACS, and PCA

NSM, as described in Richard Bejtlich's book, The Practice of Network Security Monitoring, is most effective when collection occurs at strategic network locations and utilizes a variety of methods. "Network locations" is to be understood as a logical concept, rather than only being a physical locale within geographic space. Various devices perform technical functions within and between networks, such as switches, routers, and firewalls. These devices establish logical communication convergence points, which are ideal INSM collection points. Within the CIP framework, such devices are often classified as EAPs or EACMS. To most effectively monitor BCS network traffic, EAPs and EACMs must be considered. Methods for accessing network traffic include appliances, such as physical network taps; as well as logical configuration of network devices, such as port mirroring and network flow technologies.

Monitoring authentication traffic of SIEM or PACS management system is one way to detect many attack tactics; such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The SDT acknowledges that many entities already have significant capability to detect these tactics using existing systems, such as SIEM and EDR. Adding INSM monitoring will increase the level of assurance of these important systems and may contribute to detection and incident response capabilities.

The EACMS and PACS collection scope is limited.

- This scope does not require that INSM collection be installed between a PACS system and badge readers or panels or other PACS system components.
- This scope does not require INSM collection within components of an EACMS such as intra-directory traffic or intra-SIEM traffic.

Rationale for Requirement R6 Part 6.1

Requirement R6, Part 6.1: "Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks."

Background

The SDT attempted to write very specific collection requirements, but found that it would be untenable to write regulations that would properly address collection technology for all existing scenarios and technologies. Instead, the SDT proposed that responsible entities would design an INSM collection system that provides necessary data to meet Requirement R6, Parts 6.2-6.7. Requirement R6, Part 6.1 is to be a design or architecture of the INSM system. Requirement R6, Part 6.1 allows responsible entities wide latitude to design and implement an INSM data collection system that has the highest value in their network. A common first step in designing a collection system is to perform an assessment of the in-scope network using an assessment methodology.

Assessment

There are many methodologies that could be used as a guide to analyze networks to design an effective data collection system. Legitimate methodologies have originated from physical security, engineering, military, and cybersecurity. A few of these are listed in the following table:

Name	Reference
Mitre Attack	https://attack.mitre.org/
Consequence-driven Cyber-informed Engineering	https://inl.gov/cce/
Crown Jewel Analysis (CJA)	https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis
Proprietary Analysis methods	Contact government partners or vendors

The SDT recommends that the entity select any valid methodology and use the included processes to prioritize data collection to improve upon the existing visibility and detection capabilities of the organization.

Many important considerations exist when designing data collection for an INSM system. In allowing latitude in the design of an INSM system collection the SDT had two primary concerns:

1. That Regional Entities would require too much INSM collection and force entities to move resources from other effective cybersecurity detection systems such as SIEM and endpoint monitoring to INSM collection.
2. That responsible entities would not implement enough INSM collection to provide visibility of important network-based communications.

The following sections outline considerations to find a “just right” balance of INSM data collection that improves the detection capabilities of the entity.

Design

The Design phase includes input from the network assessment and results in a description of where to deploy collection methods, which types of collection methods the responsible entity will utilize, and the data types to be collected.

The applicable environments for INSM collection have different network topologies, technologies, and support team capabilities. Collection environments differ and could include centralized environments such as control centers and generation or distributed environments such as substations. Collection technology could vary between transmission, distribution, generations, substations, renewables, and storage.

An additional consideration would be the network traffic. Control Centers may have relatively few industrial protocols (e.g., DNP3, ICCP, and Historian) with a large amount of software that is more “IT” in nature, such as databases, web services, and tiered application architectures. Substations might have no web services but a high percentage of industrial protocols such as IEC-61850, DNP3, SyncroPhasor, and

historian traffic. Variations in collection methods and tools are expected and warranted in an INSM system that provides balanced collection across various control systems.

Data Collection Methods

The following table outlines some considerations for data collection from the SDT:

Method	Comments
Network TAPs (physical devices)	Hardware costs are high. Device failure scenarios are unknown to many vendors. Deployment requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Usually not ERC.
Port Mirrors/SPAN ports **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although responsible entities will likely install network aggregators which have relatively high cost) No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Packet loss (minimal amount) is expected. Collects layer 2 and layer 3 communications. Most SPAN ports pass data at layer 2 (not externally routable communications) and therefore, may not need to traverse an EAP. Usually not ERC.
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Capable of performing in low bandwidth environments. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments. High cost for distributed environments.
SDN Networks	Central management capability often built in.

	Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have a capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.

Thorough implementation of an INSM system often results in over-duplication of communications data. Individual packets are copied each time they pass another network monitoring location. Depending on the communications path, the number of monitoring points in the environment, and endpoints involved, a single Ethernet packet could be duplicated multiple times by the INSM system. This results in reduced resource efficiency and poor INSM system performance.

Some entities may decide to implement an INSM system utilizing fewer collection points located closer to the core of the network environments. In doing so, these entities may also implement technology to remove duplicated packets at or near the collection points prior to data being sent to the INSM system. Others may choose to deploy more INSM sensors closer to the end points on access layer switches. This reduces the amount of duplication, but increases the number of monitoring points. Either method, or a combination of the two, are acceptable. Classification of de-duplication appliances would likely be as a BCSI repository unless configured and classified differently by the Responsible Entity.

Deployment time for each technology is an important consideration to achieve compliance within the implementation timeframes of this requirement.

Out of Scope collection

Requirement R6 does not require collection of data such as:

- Serial communications
- 4-20ma circuits
- Wide area network circuits such as MPLS (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used)

Relative/Generalized Implementation Timeframes of Collection Technology

To attain compliance, a responsible entity will need to implement INSM within the necessary time frame. Implementation time will need to be considered. A very generalized table below outlines considerations of implementation timeframes after the entity completes product selection, planning, and testing of data collection components. The timeframes below do not account for delays caused by seasonal maintenance windows, inclement weather, disasters, and other operational considerations.

	Control Centers	Generation Plants	Substations
Network TAPs (physical devices)	Months	Months	Years to Decades
Port Mirrors/SPAN ports	Months	Months	Months
Network Flow	Weeks	Weeks	Weeks
RSPAN	Weeks	Weeks	Depends on Bandwidth availability
Sensor Deployment	Months	Months	Years to Decades

Data Collection Methods

Part of the design considerations include specific plans of where to monitor the network, how to monitor each network collection point, and what data types will be gathered.

Consideration	Example Options
Identification of network collection points (Where to Monitor)	Network Core Network Distribution switches Network Access layers Carrier level (MPLS, etc.) Identification of network convergence points
Identification of Collection technology (How to Monitor)	Network TAPs/Prisms Mirror Ports/SPAN Ports RSPAN configurations Forwarding NetFlow data SDN traffic logs Other collection technology
Identification of Data Types (Network Data Sources)	Network Connection Creation Network Traffic Content (PCAP) Network Traffic Flow

Principles and caveats

As entities design a collection system by determining where, how, and which data sources are to be collected, regional entities and responsible entities should keep in mind several important principles and caveats related to achieving balance in INSM collection:

1. Requirement R6, Part 6.1 does not require data collection from every switch and every location on the network.
    a. As data is collected from more switches in a single broadcast domain, the amount of duplicate traffic will increase. Collecting the right data will sometimes require limiting collection points.

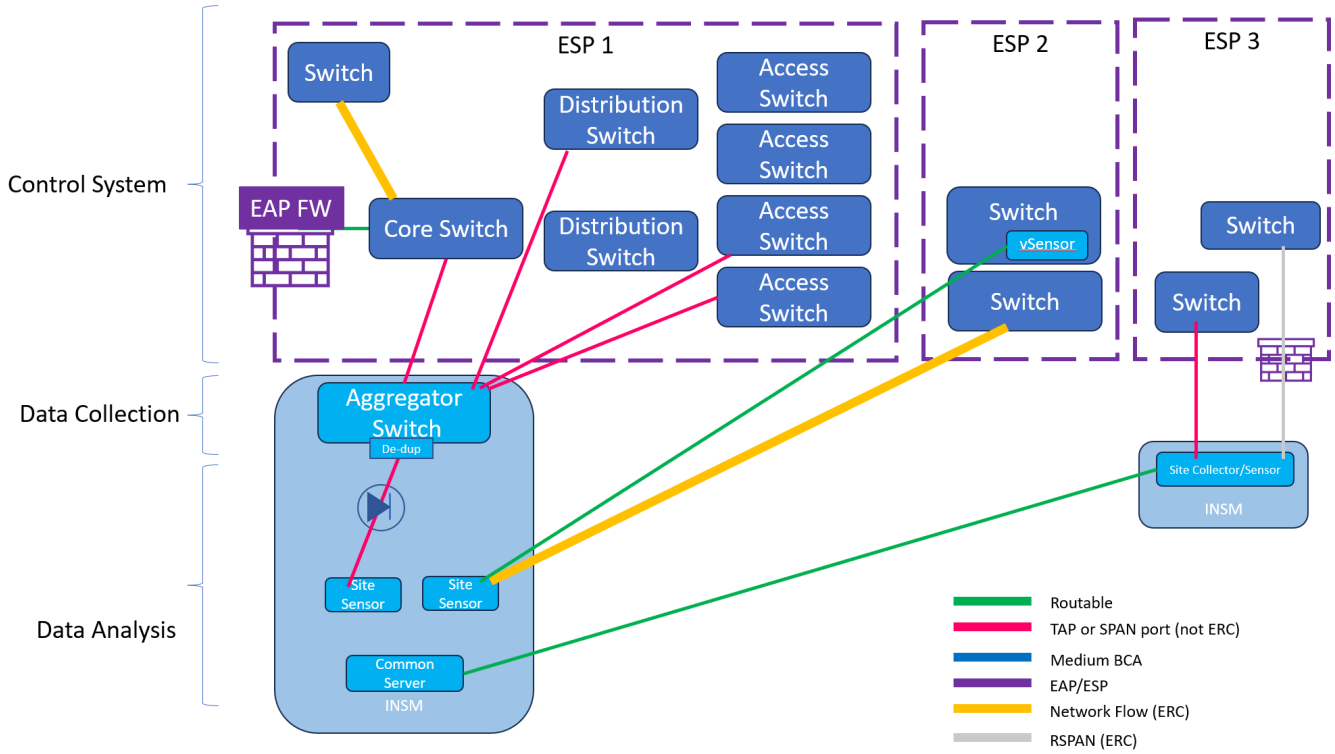
2. The entity might perform a threat assessment of adversary tactics, techniques, and procedures that have been used in attacks of other entities. This analysis might drive collection priorities to focus on targeted threats and threat vectors rather than broad collection of data with lower value.
3. A compliant low maturity INSM collection could focus on network locations and network source data that provide breadth of collection. Entities can then use this data to evaluate additional network collection points, collection technology, and data types that are needed to improve the system over time by adding or removing collection points and modifying collection methods.
4. Existing INSM products do not have the capability to identify or analyze all industrial protocols. When selecting tools to use for automated analysis, entities may choose to select data collection methods which align with the capabilities of tools and recommended by the tool vendors. Protocol identification errors do not constitute potential non-compliance.
5. Operational changes might require temporary or extended removal of INSM collection at some locations. In some situations, disabling collection or suppressing alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R6, Part 6.1.
6. Known and expected INSM limitations include:
    a. Limited analysis of encrypted traffic;
    b. High rates of false positive alerts;
    c. Wireless collection, especially in mesh networks, leads to inconsistent data collection; and
    d. Collection volume can frequently overwhelm existing analysis technology. There will exist situations when network volume reduces the visibility of network traffic. This is a known limitation of INSM technology and does not justify a potential non-compliance finding.
7. Centralized environments (control centers and generation) will likely require TAPs and/or SPAN ports to achieve balanced levels of visibility.
8. Distributed environments (substations) are more likely to deploy distributed collection, such as Network Flow or RSPAN. Entities may choose to deploy devices in distributed environments, or they may collect substation data from network aggregation points or optionally at larger substations to provide a balanced level of visibility.
9. Networks that connect to external private networks, such as turbine monitoring systems, ICCP connections, etc., are high value networks for INSM data collection and should be included in a balanced collection system.
10. Responsible entities that have mature endpoint collection and detection systems may not require as much INSM collection to achieve balanced collection, as an entity that does not collect detailed endpoint logs including memory and process logging. Existing breadth of detection can be visualized using tools such as MITRE Att&ck. Reports that demonstrate detection capability can be used to identify blind spots and to demonstrate balance.

11. An entity with mature firewall logging capabilities and extensive segmentation may choose to include firewall logs to augment INSM collection.
12. Some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a balanced approach might include a collection of firewall logs or logging communications at an upstream location rather than installing more hardware and reducing the overall reliability of the system. Alternatively, forwarding Network Flow data from routers or firewalls may be a more balanced method of collecting data.
13. Use of modern technology, such as Software Defined Networks (SDN), may provide relevant data as part of an INSM data collection system.
14. Collecting INSM data from multiple switches in a broadcast domain may result in significant data duplication. Entities may choose to collect data at locations that minimize redundant data collection (e.g., multicast and broadcast traffic) or to implement network aggregation tools that provide deduplication capabilities.
15. Filtering or elimination of traffic with low cybersecurity value (backups, replication, video, encrypted traffic, etc.) is expected in a balanced INSM collection system.

Balance in INSM collection and compliance with Requirement R6, Part 6.1 is achieved by having broad detection capability. As entities move through a maturity process, they may start with broad levels of network collection. As they mature detection capabilities, an entity that collects detailed data from endpoints and other systems may find that a reduction in network collection is justified. High maturity entities might use threat intelligence information to further refine and change data collection and focus detection efforts on tactics that have been observed and published through information sharing networks. At every level of maturity, the goal of INSM and other detection systems is to detect adversarial activity in networks and on endpoints. An entity that can demonstrate the ability to detect a broad array of adversary tactics and techniques using INSM and other systems is compliant with the intent of Requirement R6, Part 6.1.

Reference Architecture

A sample reference architecture for INSM collection and logging data is shown below. This diagram is intended to show a wide variety of possible collection methods. Entities are not expected to implement all of these, but rather to choose and implement the collection methods that provide the most value to the entity.



This reference architecture has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.

- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

The SDT acknowledges that this reference architecture does not properly represent all emerging and extremely promising technologies, such as software defined networking (SDN) and endpoint-based network isolation technologies. Entities that utilize SDN or similar technologies are encouraged to work with network vendors and detection vendors to design systems that will achieve the goals outlined in this document. SDN can provide network visibility and has the capability of preventing unauthorized network communications. Prevention capability afforded by SDN and other software-based tools is a significant step towards the goal of protecting the BES.

A properly implemented software-based detection and prevention solution may provide higher levels of protection than a passive INSM system. An entity that demonstrates a software-based solution which prevents attacks and logs the blocked network communications has met the intent of the Requirement R6, Parts 6.1 and 6.2 data collection and logging requirements. Additionally, software-defined policies that allow only authorized and expected communications explicitly meet, and exceed, the intent of Requirement R6, Part 6.3.

Technology which blocks unauthorized communication is deemed to meet the intent of Requirement R6, Parts 6.4 and 6.5 by both detecting that the communication is not authorized, and implementing a pre-defined action such as “block” or “learn.” An entity that shows example policies and the resulting network communications, as outlined above, has demonstrated compliance with these requirements.

Rationale for Requirement R6, Part 6.2

Requirement R6, Part 6.2: “Log collected data regarding network communications at the network locations identified in Part 6.1.”

Collecting and logging network traffic is a core requirement of INSM (Requirement R6, Part 6.2).

Log

When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to:

- Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic.
- Forwarding log information to a searchable database for retention.
- Summarizing logs in a searchable database.

Rationale for Requirement R6, Part 6.3

Requirement R6, Part 6.3: "Evaluate the collected data to document the expected network communication baseline."

In the context of INSM, the required network communication baseline is a record of past network communication and traffic. A baseline could include information about the traffic, such as:

- Layer 2 traffic, such as:
  - ARP;
  - ICMP;
  - DHCP requests;
  - Multicasts;
  - Broadcasts;
  - Source MAC addresses;
  - Destination MAC addresses;
  - VLAN tags; or
  - CDP/LLDP
- Layer 3 traffic, such as:
  - Source IP addresses;
  - Destination IP addresses;
  - Source TCP and UDP ports;
  - Destination TCP and UDP ports;
  - TCP header information; or
  - TCP payload metadata (size, content, determination if encrypted)
- Connection Creation information
  - TCP 3-way handshake; or
  - Connection termination information
- Summarizations of any of the above data
  - In control networks there are devices that send very repetitive data across the networks at high frequency. A summarization of this data is an acceptable part of baseline. For example, a turbine controller that continuously multicasts turbine status information at a rate of 100 multicasts per second is an example of communications that might make sense to summarize rather than to store in a raw format.
- Software and protocols in use on the network

- Some network communications can be linked to specific software with a high degree of confidence. Examples include telnet, ftp, dns, smtp, snmp, ICMP, and similar unencrypted protocols that have internet RFP standards defined. However, some network communications may require analysis to infer the software being used. It is understood that encrypted payloads using common tcp or udp ports may be difficult to identify correctly. INSM systems with accurate network communications protocol (software) classification are highly useful for cybersecurity investigations. Responsible entities are encouraged to use tools that classify the software being used, it is understood that no system will achieve 100% protocol identification accuracy.

➢ Asset information

- Network data may be used to gather information about assets communicating on the network which is useful for cybersecurity investigations. Entities are encouraged to use tools that identify assets and enrich asset data, it is understood that no system will achieve 100% accuracy of asset information from network analysis.

A baseline is …	A baseline is not …
Record of observed traffic	A spreadsheet listing all expected traffic
Continuously updated by a computer	Updated infrequently by a person
Searchable database	Point-in-time list
Assets that have communicated on the network	A spreadsheet of assets made by an intern or engineer

There are at least two justifiable purposes for maintaining this network baseline information:

1. Baseline data and network traffic is often used as a starting point when hunting for threat activity. An unusual traffic pattern or unexpected connection attempt might lead to expanded investigations through other log sources including endpoint logs, firewall logs, application logs, dns traffic, and other relevant data sources.
2. Cybersecurity analysts can search through the data to answer relevant questions related to cybersecurity investigations.

Baseline network traffic data is normally expected to be stored for an amount of time and then discarded. Depending on the type and amount of data retention, times could vary from seconds (for payload data – especially encrypted content) to several months for network connection and content summaries. Requirement R6, Part 6.3 does not include any expectation that the entity would manually create a list of all known good traffic and update that documentation at a regular interval. Instead, Requirement R6, Part 6.3 is an expectation that the entity can look at a history of actual traffic that can be used for further investigations, threat hunts, and incident response.

Note: as used here, the term *"baseline"* connotes a baseline of network traffic. This is distinct and separate from a baseline of configuration settings as used in CIP-010-4.

Rationale for Requirement R6, Part 6.4

Requirement R6, Part 6.4: "Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2."

There are many methods that can be used to monitor logs to detect anomalous activity including, but not limited to:

- Threat Hunting
- Signature based alerts
- Correlation of signatures with other logged activities
- Anomaly Detection (as defined by a software tool or vendor)
- Artificial Intelligence and Machine Learning
- Other proprietary and open-source methods

Compliance with Requirement R6, Part 6.4 will probably result in many notifications. There is no expectation in Requirement R6, Part 6.4 that every notification generated by a tool requires human response. At the beginning of an INSM implementation, many notifications can be safely ignored. With time, maturity, and tuning, the entity will likely adjust the notifications in a way that balances false positive notifications with true positive notifications which require additional analysis (see Requirement R6, Part 6.5).

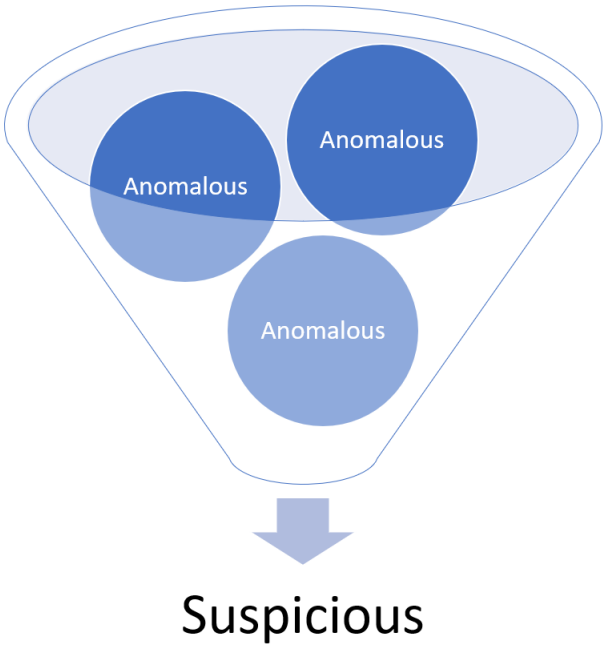
An entity may choose to comply with Requirement R6, Part 6.4 by logging all occurrences of specific events. For example, an entity may choose to alert on every connection using ssh and RDP with the knowledge that these alerts are nearly always authorized. By pre-generating events for these expected remote connections, an entity can visualize patterns that help detect unauthorized connections. These visualizations are useful during incident response investigations and threat hunting activities to help analysts differentiate between valid connections and suspicious connections. There is no justification for non-compliance with Requirement R6, Part 6.4 if entities automate generation of specific events. This is often an example of security automation and is an indicator of a proactive security process rather than a non-compliant organization.

Terminology

As used in this document and the INSM Requirement R6 and its part, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the entity might classify communications as benign, suspicious, or other similar classifications.

Unless specified, use of the word "anomalous" or "anomaly" in this document, does not refer to any proprietary technology commonly referred to as "anomaly detection."

The SDT debated using other terms and, at one point, used the term suspicious. After extended discussion and consultation with project observers, the term "anomalous" is used to indicate any notification or communication that is unexpected. As used in this document, "suspicious" is a term applied to network traffic or data after analysis has been performed on it resulting in escalation to a higher level of interest. Suspicious traffic may or may not require escalation to an incident response process, such as defined in Reliability Standard CIP-008.



It is expected that INSM systems will require constant and ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while alerts are being tuned to provide a higher signal to noise ratio.

Rationale for Requirement R6, Part 6.5

Requirement R6, Part 6.5: "One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action."

"The most important component of NSM is the analysis process. This is where the analyst takes the output from a detection mechanism (Requirement R6, Part 6.4) and accesses various data sources to collect information that can help them determine whether something detrimental to the network or the information stored on it has actually happened. The process the analyst goes through in order to accomplish this is called the analysis process." (Applied Network Security Monitoring Chapter 15)

When an organization first deploys INSM and begins analyzing the information generated by an INSM system, it would be normal and expected that the response and analysis process is ad-hoc. An ad-hoc process would meet the intent of Requirement R6, Part 6.5 for an entity without time and experience. As more time, experience, and maturity develops within an organization, the analysis process should necessarily improve from an ad-hoc state to a more formal process and procedure. Responsible entities may choose to adopt other existing analysis processes used for other cybersecurity tools, such as SIEM. A mature entity would have specific procedures, processes, playbooks, and automation to analyze anomalous network activity prior to escalation.

Compliance with Requirement R6, Part 6.5 requires some analysis be performed on the data as a starting point to detect malicious activity. This may be as simple as classifying the notification based on risk so that analysts can respond to high-risk notifications and not waste time with low-risk notifications.

An analysis methodology in a mature environment might include recurring threat hunts with hypothesis based on observed notifications or external threat intelligence.

The following are important points:

1. There is no specific response timeframe for every situation.
    a. If an entity is in the middle of investigating an active cybersecurity event and many high-risk notifications have occurred, it may be perfectly acceptable for the response team to triage high-risk or high-severity events into a "dumpster fire" category and ignore those events for hours or days while focused incident response activities occur.
2. During normal situations, it is expected that responsible entities would assess high-risk or high-severity notifications in a more-timely fashion

Confidence Level

Order No. 887 states that responsible entities have the capability to "identify anomalous activity to a high level of confidence." To achieve a high-level of confidence, responsible entities are expected to add INSM to existing detection systems and processes. INSM cannot replace other detection systems, such as SIEM or endpoint detection, but an entity might choose to add network communications information to a SIEM in order to meet the Requirement R6 and its parts, or an entity might include INSM data in an existing SIEM or similar tool.

An entity that has implemented a system that: (1) logs network traffic, (2) maintains logs and other data collected regarding network traffic, and (3) minimizes the likelihood of an attacker removing these logs, is deemed to have achieved this high level of confidence.

Rationale for Requirement R6, Part 6.6

Requirement R6, Part 6.6: "Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity."

Requirement R6, Part 6.6 allows responsible entities to choose which data to store for longer periods of time while discarding data that is repetitive or has diminishing value over time. It is expected that retention will specify longer retention timeframes of data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time.

A sample retention chart is provided below to demonstrate retention considerations:

Data Type	Cybersecurity Value over time	Retention Cost	Suggested Retention Timeframes
Full PCAP (payloads)	Value diminishes quickly with time Encrypted payloads have little to no value	High	Commonly 0-3 days Some use cases that could specify days to weeks or more if desired. Some use cases could specify no collection or retention of payload data at all. Retention is more likely to occur in centralized environments such as control centers and generation.
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Network traffic records generated as part of an analysis or investigation**	Value diminishes slowly with time	Low	If found to be evidence of a Cyber Security incident, then retention is specified by entity's CIP-008 process. If no incident was found, then retention should be aligned with the entity's data retention schedule.
Network Connection data generated from pcap **Network flow data** **Network Connection Information**	Value diminishes slowly with time	Low	Commonly 3-6 months Longer timeframes are acceptable per INSM system capability.

- The SDT notes that many tools in 2023 commonly set retention at approximately three (3) months, which is an acceptable timeframe given the threat environment and tool capability in 2023. The SDT encourages vendors to increase retention capabilities of tools to match adversary dwell time.

In many INSM tools, data retention is specified by the number of events or records of network communications that can be stored. Network traffic spikes, which are common in applicable networks,

consume a larger volume of storage space. It is expected that retention timeframes specified are moving average targets rather than absolute date values.

As the maturity level of INSM systems increase, it is also expected that data collection may be filtered to exclude data that is deemed to be of lower value. For example, it is highly likely that an entity would choose to exclude backup traffic, video traffic, replication traffic, virtual machine migration traffic, and other high volume/low value data from collection. These exclusions enhance the ability of an INSM system to analyze traffic and generally result in higher signal to noise ratios and better detection outcomes.

Rationale for Requirement R6, Part 6.7

Requirement R6, Part 6.7: "One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary."

A common adversary tactic is "Indicator Removal." The intent of Requirement R6, Part 6.7 is to protect the collected INSM data from modification or deletion by an adversary.

Suggestions for compliance with this requirement include controls used to protect BCSI and EACMS system. Some additional suggestions that should be considered to safeguard INSM data include:

- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Granting only authorized personnel access to the INSM system.
- Segmentation of the INSM system into an isolated network separate from OT and corporate networks.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Note that no part of Requirement R6, Part 6.7 is intended to limit information sharing with partner utilities, government partners, and other cyber security intelligence partners. The focus of Requirement R6, Part 6.7 is to ensure the data is available and has integrity.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through January 17, 2024
Ballot Pools Forming through January 2, 2024

Now Available

A 35-day formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Wednesday, January 17, 2024** for the following standard and implementation plan:

- CIP-007-X – Cyber Security – Systems Security Management
- Implementation Plan

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.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Tuesday, January 2, 2024.** Registered Ballot Body members can join the ballot pools 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

Initial ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **January 8-17, 2024**.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | Draft 1
Comment Period Start Date:	12/14/2023
Comment Period End Date:	1/17/2024
Associated Ballots:	2023-03 Internal Network Security Monitoring (INSM) CIP-007-X IN 1 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-007-X Non-Binding Poll IN 1 NB 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 75 sets of responses, including comments from approximately 198 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

3. Order No. 887 also references "CIP-Network Environment" that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

5. The Project 2023-03 SDT held extensive conversations about the term "baseline" and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT's use of the term "network communications 'baseline'" is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term "anomalous." The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of "anomalous" was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term "anomalous" was the appropriate term to use to describe that methodology. Do you agree that that the term "anomalous" effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

11. 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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO

					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
Anne Kronshage	Anne Kronshage			Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Southern Company -	Colby Galloway	1,3,5,6	MRO,RF,SERC,Texas RE,WECC	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
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Leslie Burke	Southern Company - Southern Company Generation	5	SERC
Jay Sethi	Jay Sethi		MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
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
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF

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
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6		Proj 2023-03 INSM	Rachel Schuldt	Black Hills Corporation	6	WECC
					Micah Runner	Black Hills Corporation	1	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Josh Combs	Black Hills Corporation	3	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC

Jeffrey Streifling	NB Power Corporation	1	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC

					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	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
	Western Electricity	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
						Morgan King	WECC	10	WECC

Coordinating Council					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
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
					Gary Dollins	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
					Jarrod Murdaugh	Sho-Me Power Electric Cooperative	3	SERC
	Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene Free	Santee Cooper	1,3,5,6	SERC
						Christie Pope	Santee Cooper	1,3,5,6	SERC
						Chris Mcneil	Santee Cooper	1,3,5,6	SERC
						Troy Lee	Santee Cooper	1,3,5,6	SERC

					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Jordan Steele	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Shedrick Snider	Santee Cooper	1,3,5,6	SERC
					Kevin Gainey	Santee Cooper	1,3,5,6	SERC
					Lachelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

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

Answer	No
Document Name	

Comment

1. The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications.

2. The standard should be focused on BES Cyber Systems and PCAs (e.g., those systems inside the ESP). Inclusion of non-BES Cyber Assets, coupled with the ambiguity of non-glossary defined criterion is overly broad and diminishes the focus on protecting the most important systems.

Likes 0	
Dislikes 0	

Response

Karen Artola - CPS Energy - 1,3,5 - Texas RE

Answer	No
Document Name	

Comment

With the increased concern of critical infrastructure infiltration by foreign adversaries, excluding low impact BCS presents a moderate level of risk and vulnerability.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and

• PCA	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) believes the proposed language does not explicitly exclude low impact BCS and medium impact BCS without ERC, it does not mention low impact. It explicitly includes applicable systems, but it does not explicitly exclude anything.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 current language in Draft 1.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees it is clear that low impact BCS and medium impact BCS without ERC are not included in the proposed requirement.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment	
NEE supports EEI comments: “EEI agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC. “	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes

Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
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 proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	Yes
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 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	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
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	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
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	
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	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
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	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
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 RSC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
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	

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

We appreciate the effort of the SDT in trying to interpret FERC Order No. 887 and revise the CIP standards to address it appropriately. We agree that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the “CIP-networked environment” diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP. PACS communication systems may be configured in such a way that it is completely separate from the OT environment. By including communication between EACMS and PACS, the standard could unintentionally be increasing the scope of many CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees that Order 887 explicitly included high impact BCS and medium impact BCS with ERC. However, the question concerns the 'cyber assets included in the standard' which is a larger scope. Given the unclear scoping of 6.1 as currently written, requirement part 6.1 itself, the diagrams showing some ‘out of scope’ PACS components, and statements in the TR that state that not all Cyber Assets involved will be of sufficient monitoring value to include, Southern Company concludes that not every Cyber Asset in the ‘CIP Networked Environment’ should be included in mandatory scope.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
It is unclear why EACMS that perform only monitoring function are excluded from the requirements. An EACMS that only monitors, such as SIEM, could be compromised should there be any deletion or modification of logs concealing the malicious activities or traffic. Thus, it should also be included in order to improve the reliability.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	

Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
While PNMR agrees with the cyber assets included within the standard, it does not necessarily believe that this requirement as a whole increases reliability but more so, security.	
Likes 0	
Dislikes 0	

Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
The question is somewhat unclear. Interpreted as if there is a subset of “scoping” besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The “scoping” mechanism is unclear when reviewing the proposed CIP-007 R6.1. It is also unclear what “will further reliability within the CIP-networked environment”. How would this be measured? Is this purely subjective? A Responsible Entity could disagree. EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.	
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 RSC

Answer	No
Document Name	

Comment

The question is somewhat unclear. Interpreted as if there is a subset of “scoping” besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The “scoping” mechanism is unclear when reviewing the proposed CIP-007 R6.1.

It is also unclear what “will further reliability within the CIP-networked environment”. How would this be measured? Is this purely subjective? A Responsible Entity could disagree.

EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	

Comment

Duke Energy notes that the defined term BCS is inclusive of devices classified as BCA and not other associated classified cyber assets, and therefore agrees with the BCS that were selected for inclusion. However, Duke Energy does not agree that the additional cyber assets included in the proposed standard’s applicability further reliability within the CIP-networked environment. We do not support the interpretation that the CIP-networked environment is inclusive of EACMS and PACS-classified cyber assets that do not reside within an ESP. Since V5 took effect, the only constructs for trust zones defined within the CIP standards are the ESP applicable for High/Medium BCS and the Low Electronic Access Controls required by CIP-003 Attachment 1 Section 3. There is no trust zone that the standards contemplate for EACMS and PACS devices that reside outside the above identified zones. Therefore, the intention to monitor east-west traffic within a trust zone in FERC Order 887 most clearly fits with the expectation that INSM is applied within applicable ESPs to increase network visibility beyond the existing perimeter-based controls required by CIP-005. Moving beyond the BCS and outside the ESP takes the focus off the most critical environments for monitoring. INSM systems are likely to generate extreme volumes of data as entities mature their implementations. Large data volumes will require significant investment of time and resources to generate meaningful baselines of network traffic, especially for large entities with diverse software solutions across their various BCS and EACMS. An unclear and overly large scope for the initial INSM implementation threatens to create alarm/alert fatigue that will hamper the ability of entities to detect and respond to threats to their most critical systems residing within their ESPs.

Likes 0	

Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

FERC Order 887 did not include EACMS and PACS. There is no requirement that EACMS or PACS be protected by a firewall, so to include them as part of "inside the CIP-networked environment" is a huge stretch for the Standards Drafting Team to make and scope creep of Order 887. Including EACMS and PACS in the requirement for INSM, where monitoring is only required between them, does not further the reliability and security inside the CIP networked environment.

There is likely to be a lot of "noise" that must be tuned out when trying to monitor only traffic between certain EACMS and PACS devices since they can be inside more open networked environments. The security value of monitoring only the "INSM" (east-west) traffic assumes that you must first be compromised by non-INSM (north-south) traffic before you would potentially see anomalous INSM communication; this makes very little security sense.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

Likes 0	

Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The "CIP-networked environment" diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS, and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	

Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
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 is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the question refers to CIP-networked environment, which has created confusion about the SDT’s goal for responses. To refer to a CIP-networked environment high impact BCS and medium impact Cyber Assets with ERC does not align with current CIP-005 language in R1.1 which requires medium and high impact BCS and their associated Protected Cyber Assets “connected to a network via a routable protocol shall reside within a defined ESP.” Inclusion of EACMS and PACs in the standard draft language goes beyond Order No. 887.	
Likes 0	

Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI is of the opinion that the proposed changes will improve the security of the CIP-networked environment. “	
Likes 0	

Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 cyber assets included within the standard will further reliability within the “CIP-network environment”**.**	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes R6.2 could conceivably lower security posture if the transport and/or repository of such logging information is compromised.	
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	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
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	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Keele - Entergy - 3	
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	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
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	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	

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	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes that whether any other ballot pool member agrees with the directives in Order 887 is moot. Questions about what types of BCS should or should not be addressed by revisions to one or more CIP Standards should have been raised after FERC issued its Notice of Proposed Rulemaking about INSM on January 27, 2022.	
Likes 0	
Dislikes 0	
Response	

3. Order No. 887 also references "CIP-Network Environment" that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The scoping of PCA is clear. However, the language "that perform access control functions" is not clear. The language would be improved by specifying what type of "access control functions" are applicable (e.g., for authentication). Consider the following revisions for the High and Medium Impact scoping language in the Applicable Systems section:

1. EACMS that perform authentication functions;

2. PACS that rely upon EACMS that perform authentication functions; …

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications.

As the standard in current state does not direct that PACS be protected by an EACMS, entities are dis-incentivized to protect PACS due to the additional regulatory exposure created by the draft language.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	
Comment	

While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.

Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	
Response	

Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don’t feel the term CIP-Network Environment should be used here when it can’t be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn’t where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be

subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA supports Chelan PUD's remarks proposing modification of the draft scoping language in the Table R6 – INSM - Applicable Systems section to reduce confusion about which EACMS and PACS are in scope: 1. EACMS that perform authentication functions; 2. PACS that rely upon EACMS that perform authentication functions; …" For clarity, BPA also recommends the drafting team reinstate the definitions pertaining to "Applicable Systems" on page 6 to include definitions for any new terms used in the next draft, especially the phrase "PACS that rely upon…"	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The Standard Drafting Team has done a very good job at identifying additional components in the "CIP-Network Environment" that need to be monitored without increasing the scope further than necessary. The technical rational describes the scope, including a diagram. The language used in the applicability section EACMS "that performs access control functions" does not match the diagram and intent of the Standard Drafting Team. This phrase would include all access control EACMS, including the following that were marked as out of scope on the diagram: An EACMS that contains an EAP, for example a firewall	

An EACMS that acts as an Intermediate System, for example a jump host

To clarify the EACMS in scope it is suggested to use the wording “EACMS that perform authentication for more than one CIP Cyber Asset”. This better matches the diagram presented, where traffic going to a firewall (an access control EACMS) is out of scope, however traffic to a two factor authentication server or active directory server would be in scope.

Manitoba Hydro suggests removing PACS from the applicability section, as there are no other network security requirements that apply to PACS. Traffic from EACMS that support PACS would already be included if the EACMS was in scope.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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

PG&E does not agree the language clearly indicates what is in-scope and out of scope. The FERC Order was for “internal” communications, but the current language does not clearly indicate this and could be interpreted by auditors to include traffic outside of the ESP, such as those to PACS and EACMS outside of the ESP. PG&E recommends to clearly indicate that communications outside of the ESP to devices such as PACS and EACMS are not in scope.

Likes 0	

Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Texas RE is concerned with scoping EACMS to only those that perform access control in Requirement R6. Certain monitoring systems, such as a SIEM, may be an attack priority and should be included in internal network monitoring. SIEMs contain logs for all CIP networked devices configured to send applicable security logs to them. An attack against the SIEM could subsequently result in an attacker removing logs of their activity in order to prolong time to discovery and hinder recovery efforts. Texas RE recommends removing the language "that perform access control functions" from the Applicable Systems column. Texas RE noticed the SDT identified “PACS that rely upon EACMS that perform access control functions” as an Applicable System in Requirement R6. Texas RE requests clarity on what this is intended to be mean. Texas RE noticed the technical rationale document states “CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device is out of scope.” (Page 6). The technical rationale should not create or modify requirement language. If these types of communications are intended to be out of scope, this should be represented in enforceable requirement language, either by explicitly defining what communications are in scope or by explicitly defining what communications are out of scope.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	

Comment
The order does not specifically reference EACMS and PACS, therefore it is not part of the CIP-network environment.

Likes 0	
Dislikes 0	

Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	
Comment	
Oncor stands in agreement on the comments made by EEI that states: "EEI remains concerned that the applicability section for Requirement R6 is not sufficiently clear and needs additional work in order to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested some edits to the applicability section in our response to question 4, further work may still be needed beyond replacing “access control” with “authentication control”. Nevertheless, we do feel authentication control is superior to access control, as proposed."	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with MRO provided comments: "While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS). Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed."	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No

Document Name	
Comment	
FERC Order 887 references a CIP-Network Environment in the context of assets within an Electronic Security Perimeter. The Order does not mention PCA, EACMS, or PACS. The standard language including those devices is a significant expansion of the scope of the FERC Order. While PCA are, by definition, within the Electronic Security Perimeter, EACMS and PACS are not necessarily located within the ESP and should not be included in the standard.	
Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	
Comment	

As documented in FERC Order 887, "INSM is a subset of network security monitoring that is applied within a “trust zone,” such as an electronic security perimeter. For the purpose of this rulemaking, the trust zone applicable to INSM is the CIP-networked environment," the trusted zone protected by a firewall. Including EACMS and PACS, which are not required to be protected by an ESP, Electronic Access Point (EAP), or required to be in a “trust zone” does not align with intent of the SAR or the FERC Order, which is to perform network monitoring of traffic between devices ***within*** a trusted zone.

The intent of the SAR was to close the gap that currently exists in CIP-005, which is the inability to detect lateral movement of a compromised system. The way the requirements are currently scoped, EACMS and PACS are included when they are not even required to be in a trusted zone, and only traffic between them proposed for monitoring. Therefore, this becomes a detective control to determine if a device has already been compromised.

EACMS and PACS should be removed from the project scope and the INSM requirements should be moved to CIP-005. Including EACMS and PACS in the scope, significantly increases the cost and complexity of the INSM requirement as many PACS are spread throughout different geographical locations and networks, significantly increasing the cost and complexity of implementing the requirements, with little security benefit to gain since any attack would likely come from a Cyber Asset that is not classified as an EACMS or PACS. SMUD recommends removing EACMS and PACS from the project scope and moving the INSM requirements to CIP-005 as a network and BCS level control rather than leaving it in CIP-007 where Cyber Asset level controls are typically required.

Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	

Duke Energy's understanding of the CIP-Networked Environment and its use in the order was that it meant to capture High BCS and Medium BCS without ERC, while using language that could align in the future with the requirement for Lows for which there is no ESP. With that disclaimer, we believe that the applicability clauses " EACMS that perform access control functions" and "PACS that rely upon EACMS that perform access control functions" is meant to convey a subset of EACMS and PACs, and it is unclear exactly which subset of these assets is intended to be included. This applicability will necessitate entities performing subclassifications of their EACMS and PACS to determine potential scope. We recommend the Applicable Systems be scoped to High Impact BES Cyber Systems and their associated PCA and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA. If the SDT is unable to align to this approach that leverages the existing CIP-required trust zones, we would request that the SDT invest the necessary time to define terms to clearly articulate which subsets of EACMS and PACS are relevant for this standard.

Likes 0	
Dislikes 0	
Response	

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	

Without discouraging implementation of ISNM, the administrative burden of classifying the NERC-defined term of EACMS more granularly diminishes the value the SDT intended. The reliability gained by requiring INSM on this subset of systems does not outweigh the increased cost or additional documentation needed to prove compliance.

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	

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI comments: " The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project. "	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment
NST believes Order 887 is clearly intended to apply exclusively to high or medium impact BCS inside ESPs, its use of the phrase, "CIP-networked environments" notwithstanding. There is no mention in the Order of "CIP" devices that may be outside ESPs, such as EACMS and PACS, and we believe this was in fact intentional. We note, further, there are numerous statements in the Order that reinforce this opinion, including: "INSM is a subset of network security monitoring that is applied within a 'trust zone,' such as an electronic security perimeter." (Paragraph 2) "We find that, while the CIP Reliability Standards require monitoring of the electronic security perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack." (Paragraph 3) "Finally, INSM provides insight into east- west network traffic happening inside the network perimeter, which enables a more comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone." (Paragraph 13) "The NOPR explained that including INSM requirements in the CIP Reliability Standards would ensure that responsible entities maintain visibility over communications between networked devices within a trust zone rather than simply monitoring communications at the network perimeter access point(s) (***i.e., at the boundary of an electronic security perimeter as required by the current CIP requirements***)." (emphasis added) (Paragraph 14) "While the CIP Reliability Standards require monitoring of inbound and outbound internet communications at the electronic security perimeter, the currently effective CIP Reliability Standards do not require INSM *within* trusted CIP-networked environments for BES Cyber Systems." (Paragraph 20) In addition, the Q2 2023 issue of the highly respected and widely consulted ReliabilityFirst newsletter, "The Lighthouse," is titled, "Preparing for Internal Network Security Monitoring (INSM)." It opens with the following statements: "Internal Network Security Monitoring, or INSM, is the practice of understanding what is going on inside your networks. For the purposes of the CIP Standards, that means understanding what network traffic is occurring ***within*** your Electronic Security Perimeters (ESPs)." (emphasis added). With all due respect to the SDT's "risk-based approach" (not described in the Technical Rationale document) to deciding certain types of CIP devices outside of ESPs should** be in scope, NST believes the drafting team has far exceeded the authorization granted by the Standards Committee's approval, on August 23, 2023, of the INSM Standard Authorization Request. ** NST notes that on Page 5 of the Technical Rationale document, the SDT states, "The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) ***shall*** be inclusive of the following (adjusted for clarity for the purposes of showing SDT development of revisions to CIP-007-X):" (emphasis added). We assume the use of the word, "shall" was unintentional.

Likes 0	
Dislikes 0	

Response

Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No

Document Name	
Comment	

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	

Comment
Need to clarify which EACMS provide “access control” only. Consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”. Also please clarify that only authenticating EACMS need to be included or update the language under Applicable Systems to explain.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3	
Answer	No
Document Name	

Comment
Entergy has concerns regarding the Applicable Systems of the proposed standard and the use of new terms and/or scope increase, in particular with “PACS that rely upon EACMS that perform access control functions”. It is not clear on what “rely” means in this context. Additionally, this would expand scope beyond network security requirements for PACS, or incentivize entities to reduce security for compliance margin. For example, under the existing CIP-005 standard PACS are not required to reside in an ESP or have their External Routable Connectivity flow through an Electronic Access Point on an EACMS. Under this standard an entity could utilize a non-CIP interface on a EACMS with a segmented network to provide perimeter protections/access control as a best security practice, but this would be outside CIP-005 scope. With the proposed standard as drafted because that EACMS is providing security controls to the PACS, even though not required by CIP-005, the PACS would be brought into scope of this standard. This could incentivize entities to move PACS away from EACMS systems providing access control to less secure pathways totally outside CIP scope to avoid an increase in compliance requirements.

Likes 0	
Dislikes 0	

Response

David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	

Comment
A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS.

Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review. Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be: Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that the devices (e.g. PCA, EACMS, and PACS) are included or excluded for INSM data collection consistent with Order No. 887. Question 3 indicates “The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets” which appears to be missing a part of the statement. How did the SDT team risk-based approach exclude EACMs and PACs that are only performing monitoring functions? As described in the technical guidance, “Threat actors commonly take steps to hide their actions, and very often need to work for an extended period within targeted environments to develop disruption capabilities.” In either case, the NAGF would refer the SDT back to Order 887 in that the network traffic in scope for INSM is communications within an ESP between other Cyber Assets within that “trust zone” also referred to as east west traffic. The inclusion of EACMS and PACS goes beyond the scope of INSM and the current Draft 1 creates confusion as to the intent of the requirements commingling “Network Security Monitoring” principles which include devices outside of the ESP or “trust zones”.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	

Tacoma Power does not agree with the addition of EACMS and PACS to this Standards Project. While Order 887 specifically calls out the “CIP-Networked Environment”, there is no mention of EACMS or PACS in the Order. In reviewing previous FERC Orders that have applied to EACMS and PACS, these system types are specifically identified within the Order, see FERC Order No. 850 as an example.

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 RSC

Answer	No
Document Name	

Comment

Is this question asking to “scope” the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?)

Please clarify if the evaluation approach is CIP-007 R6.1 “…Collection methods should provide security value to address the perceived risks.”

Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing.

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don’t feel the term CIP-Network Environment should be used here when it can’t be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn’t where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	

A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS.

Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review.

Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be:

Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.

Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

Is this question asking to "scope" the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?)

Please clarify if the evaluation approach is CIP-007 R6.1 "…Collection methods should provide security value to address the perceived risks."

Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing.

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn't clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don't feel the term CIP-Network Environment should be used here when it can't be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn't where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the "CIP-Network Environment" then it should be out of scope as well.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer	No
Document Name	

Comment

The definition for EACMS currently reads, "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." PNMR understands the STD's intent to focus on EACMS designed for access control, but specifically designating types of EACMS (and PACS) for the Applicable Systems seems to indirectly change definitions. This change also deviates from all existing "Applicable Systems" in current Standards.

Additionally, to more closely align with language related to other "Applicable Systems" in other requirements, PNMR believes the "Applicable Systems" should read, "EACMS with access control functions."

Finally, PNMR is unclear on the exact meaning behind, “PACS that rely upon EACMS that perform access control functions.”	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	

Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	

We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the “CIP-Network Environment” then it should be out of scope as well.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Please see LCRA’s response to question 2 above. The term “CIP-networked environment“ is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

The EACMS that perform only monitoring function should also been included. Although described in technical rationale, it is better to properly add "CIP-Network Environment" in NERC's glossary of terms.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The FERC order specifically addressed High and Medium-Impact assets. Extending the proposed standard to associated EACMS and PACS exceeds the scope of the FERC order and they should be removed. GSOC believes that the order as written could include communication between High or Medium assets and their corresponding PACS/EACMS. Nevertheless, there is a lack of clarity regarding the inclusion of ALL EACMS and PACS communications within the Applicable Systems. If the intent is to capture such communications, this can be feasibly achieved through tools already monitoring the High and Medium assets from within their ESP.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Please see LCRA’s response to question 2 above. The term “CIP-network environment“ is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Consider defining "CIP Networked Environment" in the glossary of terms or the standard itself. Additionally, "CIP Networked Environment "could be further defined to make it clearer on what is included and excluded.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887. CEHE believes that the use of "EACMS that perform access controls" and "EACMS" from the "Interpretation of the CIP-Network Environment" diagram presented in the SDT webinar is unclear. "EACMS" seems to refer to authentication mechanisms, but EACMS in some environments, if not most, refer to firewalls that do not perform authentication, but do perform access control. CEHE suggests using the phrase "EACMS that perform authentication functions" as it relates to the "CIP-Network Environment."	
Likes 0	
Dislikes 0	

Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the comments by EEI. Additionally, Southern Company would like to state a concern for the record that the scope of the current draft does not clearly align with what is stated in the Order and the SAR. The only reference to EACMS and PACS in the Order is in section 21 and is in relation to the existing requirement CIP-007 R4.1.3. While it is clear in the Order that the scope of CIP-networked environment extends beyond the Electronic Security Perimeter, it would be helpful to industry in the future if all applicable Cyber Assets intended to be included were clearly stated in the Order and the SAR.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE believes that “PACS that rely upon EACMS that perform access control functions” is not entirely clear. It is not clear what “rely upon EACMS that perform access control functions” means. It could be interpreted to mean the PACS relies on the EACMS to validate that an individual is allowed to have physical access to a NERC CIP area, or it could be interpreted to mean the PACS relies on the EACMS to validate a username and password in order to log into the PACS server/system. SIGE would like to see further clarification included.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.

Likes 0	
Dislikes 0	

Response

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the Technical Rationale, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. We don’t recommend using the term CIP-Network Environment when it can’t be found in the glossary of terms. The diagram in the Technical Rationale is required for clarity on what the applicable systems are, but is still ambiguous enough that it leaves too much interpretation between systems that an entity identifies as applicable versus what an auditor would identify as applicable systems.

Stating that 100% coverage is not required without providing a minimum threshold or other guidance on an acceptable level of coverage leads to potential confusion. Different entities define and evaluate acceptable levels of risk differently. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is responding in support of the comments provided by EEI.

Likes 0	

Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	No
Document Name	

Comment

Prior CIP SARs have scoped a projects applicable system(s) by what is stated in the Project Scope section of a SAR. To rely on the undefined term “CIP-Network Environment” to further scope this project creates confusion for industry. The project scope of the SAR only listed –

The Standard Drafting Team (SDT) will create or modify the Reliability Standards and associated

definitions as necessary to comply with the FERC order. The scope of the project will include:

• All high impact BES Cyber Systems, and

• All medium impact BES Cyber Systems with ERC

The scope of the project should not extend to:

• medium Impact BES Cyber Systems without ERC or

• low impact BES cyber systems

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Constellation has no additional comments.

Kimberly Turco on behalf on Constellation segements 5 and 6

Likes 0	

Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 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	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Flanary - 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	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC). In addition, MISO asks the SDT to consider adding the term "CIP-networked environment" to the NERC Glossary. As this term is used in FERC Order 887, defining it could be useful in identifying which EACMS (e.g. those used for authentication only and traversing the EAP) are applicable.	
Likes 0	
Dislikes 0	
Response	

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	No
Document Name	

Comment

To avoid numerous interpretations of if '100 percent coverage is not required' then what is required. Consider the following -

'Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets, as determined by the Responsible Entity, to monitor and detect anomalous activity. Collection methods should ensure visibility to identify known or suspected malicious communications.'

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is responding in support of the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

We agree that it is clear the way Requirement R6.1 is written that not every CIP network interface is required to be monitored with INSM. However, without providing a guidance document on what provides “security value” and is considered “critical” there is enough ambiguity that there can be disagreements between what an entity has identified within its own processes and procedures and what an auditor considers to be “critical” and provides “security value”, leading to the auditor issuing PNCs. How can an auditor or entity determine they did enough?

If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.

Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments filed by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an

example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees with the comments by EEI. In addition, Southern Company offers the following comments:

Requirement R6.1 currently has an abundance of phrases that entities must prove with evidence. For example, it can be read that the entity must describe how *each* collection location or method can monitor and detect anomalous activity and specifically all connections, devices, and network communications.

Southern Company suggests 6.1 be rewritten so that it does not force entities to “prove the negative” of the gap between what they did monitor and the 100% of all applicable Cyber Assets. The following wording is recommended to align with this concept:

"One or more process(es) to identify network data collection locations the Responsible Entity determines provide sufficient security value in determining anomalous activity." With this wording concept, the evidence burden shifts to providing a reasonable monitoring location identification process and then evidence it was followed.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
CIP-007-X, Requirement R6, Part 6.1 indicates 100% is not required. This statement leaves a lot open for interpretation by an auditor. If an entity is collecting 50% of the data is it compliant or will an auditor determine this is not enough. Without a firm number communicated to auditors and entities it would be difficult to ensure Part 6.1 is interpreted the same way.	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity's interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the language is still too vague to sufficiently inform LCRA's determination of the level of coverage necessary for compliance with the requirement.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Part 6.1 includes "network communications." However, the term introduces ambiguity as it is unclear which specific network communications require identification, such as protocols, ports, applications, or other elements. The mandate for 100% coverage is not explicitly stated, creating uncertainty about the extent of coverage required. There is a lack of clarity in defining the parameters or criteria determining the necessary coverage.	

The statement, "Collection methods should provide security value to address the perceived risks," prompts questions about the nature of the perceived risks. It raises considerations about whether it necessitates the formal execution of a risk assessment specifically targeting internal networks. Additionally, there is uncertainty about the expectation to document identified risks and articulate how an entity's data location and methods effectively mitigate these risks, extending beyond the implementation of INSM (Industrial Network Security Monitoring).

The measures proposed in the Standard imply that the sole requirement is the provision of architecture documents or similar documentation. If this interpretation is accurate, the language within the updated Requirement could be simplified to explicitly state, "Identify network data collection locations and methods designed to offer visibility of network communications (excluding serial) among relevant Cyber Assets." This modification would enhance precision and eliminate potential misinterpretations.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

It is not clear to the intent. “what is more critical to monitor” and “security value to address the perceived risks” is vague; additional details/specifics should be provided.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity’s interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the language is still too vague to sufficiently inform LCRA’s determination of the level of coverage necessary for compliance with the requirement.

Likes 0	
Dislikes 0	

Response

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	No
Document Name	
Comment	
AZPS does not believe the current language is clear in regard to performing an assessment of applicable CIP network communication and determination of what is most critical to monitor. AZPS recommends “Perform an assessment to identify locations and methods to collect network communication data (excluding serial) between applicable Cyber Assets, including connections, devices, and routable protocol network communications, to monitor and detect deviations from a normal network communications baseline. Identified locations and methods are not required to provide 100% coverage, but rather should be determined based on risk, criticality and security value.”	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for	

registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS that perform **authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS that perform **authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs).** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment

EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that "100 percent coverage is not required". The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of "networks" where there is no monitoring technology available. To address this concern, we suggest adding "routable protocol" prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Requirements

Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	

Comment

The intent does not seem to be reflected in what is written. The sentence, "100 percent coverage is not required" opens too many avenues for vastly different interpretations across industry. If the intent is for an entity to design how it will collect network data in a balanced manner with criticality in mind,

then it should be stated. The “100 %” sentence could be replaced with, “Determine which CIP network communications are most critical to monitor. The monitoring and collection methods should provide security value to address the perceived risks.”

Perhaps a different approach could be to clarify that the objective is not to monitor the endpoints. The language could state that 100% of monitoring endpoints in not required.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

Comments: Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. **100 percent coverage is not required.** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a “bump in the wire” tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do. It is clear that 100% coverage isn’t required, but what provides “security value” and is considered “critical” isn’t. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
"See comments submitted 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 RSC	
Answer	No
Document Name	
Comment	
Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a "bump in the wire" tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do. It is clear that 100% coverage isn't required, but what provides "security value" and is considered "critical" isn't. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	

While the current wording mentions that "100% coverage is not required", that leaves the possibility for an auditor to demand an arbitrary amount that is less than 100%. The SRC recommends adding verbiage indicating that the collection locations and methods should be commensurate to the risk posed as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike

Answer	No
Document Name	

Comment

Tacoma Power does not agree that the intent is clearly expressed in the language of Requirement 6 Part 6.1. The term "perceived risk" is not a well-defined or measurable quantify and as such, would be difficult to implement. There is no definition within the Requirement language that clarifies what "internal" means in the internal network security monitoring term. Tacoma Power suggests defining internal network security monitoring.

Tacoma Power suggests the following for the language of Requirement 6 Part 6.1:

"Identify network data collection locations and methods that provide visibility of network communications (excluding serial) within the network subnets of applicable CIP Systems, to monitor and detect anomalous activity, including connections, devices, and network communications between applicable CIP Systems.

Note: While complete coverage is not required, the implemented collection methods should increase the probability of detecting an attack that has bypassed network perimeter-based security controls."

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The NAGF recommends that the SDT change Requirement 6.1 to state, "Identify network data collection location(s) and methods required to internally monitor applicable CIP networked environments that provide security value to address organizational risks."

Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP is concerned with the anticipated scope of Part 6.1 and believes the language should allow more flexibility for Responsible Entities to determine the network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity. SPP proposes the following language for Part 6.1: Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous network activity indicative of an attack in progress.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
The standard as drafted provides the latitude for entities to “identify network data collection locations and methods” as the first sentence of the question states. However, there is no identification in the standard of the expectations of entities to “perform an assessment” and “determine what is critical to monitor” as the second question of the sentence implies. If this is the expectation to assess and define, and entities will be audited against that assessment and definition, then it should be clearly detailed as an expectation in the standard.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. However the phrase (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. Suggest continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent.	
Likes 0	
Dislikes 0	
Response	

Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	
Comment	

NST believes the statement in the “Requirements” column of proposed Part 6.1, "100 percent coverage is not required," would almost certainly be both difficult to understand and difficult to audit. We note that the SDT addressed these concerns during the January 3, 2024 INSM webinar and provided a good explanation of what "percent coverage" was intended to mean (paraphrasing, a Responsible Entity's most important obligation is to design a collection system capable of detecting potentially malicious traffic on network segments between in-scope Cyber Assets, and so long as this is accomplished, it should be possible to justify not monitoring outbound and inbound traffic on every port on every device, which in some instances could be technically infeasible and/or prohibitively expensive). NST suggests either (a) deleting the "100 percent" statement, along with the one that follows ("Collection methods should provide security value to address the perceived risks.") or (b) moving them to the "Measures" Section of 6.1 if the SDT feels it is an important thing for Responsible Entities to understand.

Likes 0	
Dislikes 0	
Response	

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	
Comment	

“ EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that “100 percent coverage is not required”. The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of “networks” where there is no monitoring technology available. To address this concern, we suggest adding “routable protocol” prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS devices that **perform access control functions** authenticate for other CIP Cyber Assets; **and**

{C}**2. PACS that rely upon EACMS that perform access control functions; and**

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS devices that authenticate for other CIP Cyber Assets; **and**

{C}**2. PACS that rely upon EACMS that perform access control functions; and** {C}3. PCA. **Requirements** Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) **between applicable Cyber Assets** to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications. **100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.** “	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
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	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD proposes the following two options to improve Requirement R6 Part 6.1**:** “Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications, **as determined by the Responsible Entity**. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.” Or “**As determined by the Responsible Entity,** identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.”	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	

The statement "100 percent coverage is not required." does not provide sufficient clarity on what, or how much must be collected. The next statement, "Collection methods should provide security value to address the perceived risks.", appears to try and qualify this, but still does not provide a sufficient guidepost for measuring compliance. Additionally, 'coverage' is not defined and further adds to the ambiguity.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Although NIPSCO agrees with the SDT's intent, "100 percent coverage is not required," seems ambiguous. This statement does not seem necessary in the language of the Standard as the Applicable Systems table defines the scope. This should be added to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
The language in Part 6.1 is a rogue auditor's dream. If 100 percent is not required, then what percentage is acceptable and who gets to decide? If collection methods "should provide security value to address the perceived risks", then who gets to define "security value" or "perceived risks"?	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
Tri-State agrees with MRO provided comments: "The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent. Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome."

Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	

Comment
Oncor stands in agreement on the comments presented by EEI that states: "EEI does not fully support the proposed language in Requirement R6, Part 6.1. Among our concerns is the statement that "100 percent coverage is not required". While we appreciate the intent of this language, we feel it is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that simply identifying network communications may not be sufficient because there are types of "networks" where there is no monitoring technology available. To address this concern, we suggest adding "routable protocol" prior to network communications throughout R6. To address EEI's concerns, we offer the following edits in boldface below: **Applicable Systems** High Impact BES Cyber Systems and their associated: {C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**; {C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and {C}3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: {C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**;

{C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network **communications**. **100 percent coverage is not required.** Collection locations and methods should provide security value to address the perceived risks**, as determined by the responsible entity**."

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

If a Responsible Entity (RE) is found non-compliant during an audit due to ambiguous and non-quantifiable standard language, the fines could result in money being spent paying a fine that would negatively impact security elsewhere through no fault of the RE.

“100 percent coverage is not required” is ambiguous, so compliance would be met if 99.9 % coverage were achieved, and it would also be achieved at 10% IF the collection methods provide security value to address the “perceived risks”.

It doesn’t matter if the RE has 100% coverage if the RE does not “perceive” any risk or does not know how it is defined or measured. Likewise, if the RE only has 10% coverage.

What is the intention of the regulation? A RE could log every single bit of every communication and alert on every single ‘anomalous’ behavior and if the RE is not “perceiving” a risk based on some objective measurement methodology or standard, the RE is neither reducing risk nor being compliant.

Since “perceived risks” does not appear to be in the NERC Glossary of Terms, how should it be defined, and whose, or what, perception is the standard by which the compliance is measured? By the RE’s, the auditor’s or the industry, or maybe it could be any of them? This should be better defined.

We do not provide any language modifications and recommend the SDT completely review this requirement part to develop minimum quantifiable measures for compliance and utilize existing glossary terms or develop glossary terms that can be used for this requirement.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
This requirement should be broken down into two parts. One for identifying applicable network communications, and the other for identifying monitoring methods.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	No
Document Name	
Comment	

Black Hills Corporation does not fully support the proposed language. Black Hills Corporation agrees with the comments provided by EEI, “EEI does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;
2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and
3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;
2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and
3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. *(remove "100 percent coverage is not required.")* Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**."

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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

PG&E does not believe the intent is clear for Part 6.1. PG&E recommends in addition to the "100 percent coverage not required", an additional clause be added that this should be a risk-based approach, as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	

The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	
Response	

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA recognizes and appreciates the SDT's effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors, which in this case could be about what percentage they cover and what they consider anomalous activity. BPA suggests that R6.1 be rewritten to more clearly specify the requirement, such as "Use a risk-based assessment methodology to identify network data collection locations…" Language used elsewhere in the CIP Standards, such as "as determined by the Registered Entity", could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc.

BPA also suggests the final sentence ("100 percent coverage is not required…") could be incorporated into the Technical Rationale rather than the requirement.

Likes 0	
Dislikes 0	
Response	

Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	

It is clear that 100% coverage isn't required, but what provides "security value" and is considered "critical" isn't. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements.

It is clear that 100% coverage isn't required, but what provides "security value" is not. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.

Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.

Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

As written, R6 P1 is vague and will cause significant disagreement between entities as to what is considered sufficient "methods" to determine what must be collected. There is no existing standard within the cyber security practice on what precisely would constitute an effective level of data collection. While the drafting team states in the Technical Rationale that "Regional Entities would require too much INSM collection and force entities to move resources from other effective cybersecurity detection systems such as SIEM and endpoint monitoring to INSM collection", nothing about the standard itself places limits on interpretation by the RE such that what becomes deemed acceptable during audits is de facto direction by what the RE's want. For example, if during implementation it is determined that coverage of a selection of key devices is most appropriate and such selection of devices represents 75% of devices within a network because that is assessed to be the correct level of monitoring in a method, what constrains the RE from declaring the analysis to be insufficient?

In the Technical Rationale on page 8, it refers to examples of determining "assessment". However, the items listed as examples are not assessment tools to drive determination of what, precisely, should be collected at a per-packet level. Use of the MTIRE ATT&CK Framework is simply a taxonomy to "talk" about different stages of a cyber-attack and, notably, how to associate those terms with documentation. Two organizations using the ATT&CK framework will have substantively different interpretations of what a taxonomy element means and how it should be used, if at all. One entity's definition may not match an RE's definition and thus conflict will arise during audit. The Technical Rational does not solve interpretive differences, in fact it enhances them.

Another example of the problems with interpretation and execution is table of methods on pp 9-10 and combined with the reference diagram on page 14. The references are overly simplistic and not necessarily relatable to in-the-field deployments of network infrastructure. The "data collection" is

referred to as a “TAP or SPAN” off a series of various switches or, in a few cases, “Network Flow”. However, each label over-simplifies a significantly complicated series of engineering decisions. For example, most switches that are not large carrier-class devices, cannot effectively tap every single port and span/repeat those packets to another location. There are significant issues with processing power available on control planes of network devices, many of which will degrade the operational performance of devices if not carefully limited. Other proposed technologies, such as sFlow, are not security protocols. sFlow is, specifically, an industry protocol that was created to sample traffic moving through an interface for the purposes of calculating bust-based bandwidth billing (e.g., calculating the 95% percentile traffic for rate billing, etc.). The reference architecture also creates an interesting chicken-egg scenario, in combination with R6 P7, where monitoring assets will themselves become assets that require monitoring. At the end of the day, the requirement and all associated rationale is very subjective and will lead to significant interpretive differences and clashes. If the SDT is not going to mandate 100% coverage – and all pervious CIP standards essentially require 100% coverage within a given set of “Applicable Systems” listed in the part – then the decision points need to be clear so that all entities can agree on reasonable interpretations of inclusivity within a defined set of boundaries.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	

NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	No
Document Name	

Comment

Even though the Requirement states "100 percent coverage is not required", this requirement is too subjective and open to different interpretations and implementations; this could prove difficult in providing adequate evidence in an audit. Suggested language for 6.1 is as follows: "*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.*"

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	
Comment	

The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

It is unclear what type of data is to be collected. Suggest revise to define expectations for what type of data should be collected. There is no minimum threshold for acceptable INSM coverage. Suggest revise to clearly define what type of data is to be collected, and establish a minimum threshold for what INSM coverage is acceptable. The undefined term "connection" is unclear in context. Suggest define what is meant by this term.

Consider leveraging the OSI model to clearly identify the target depth of monitoring. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.

Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	
Comment	

There are really two things being asked here: (1) perform the assessment to determine what is most critical to monitor and (2) identify the locations and methods to perform the monitoring. As written, it is not clear that both are being asked. So, this requirement either needs to be rewritten or broken up into two parts. It could be rewritten as “Assess network communications (excluding serial) between applicable Cyber Assets to determine the most critical communications and identify network data collection locations that monitor and detect for anomalous activity.”

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	Yes
Document Name	

Comment

The last sentence, which refers to security value to address the perceived risks, is highly vague. It is not clear how an auditor would verify what is the perception of risks for an entity or the security value.

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has no additional comments

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the current language in 6.1 is clear to the intent that every network interface will not have to be monitored. Entities should consider however, that this approach will require they have a consistent rationale for what is included and be able to defend communications that fall into scope but were not selected for inclusion.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
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	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #4.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	
Document Name	
Comment	
Texas RE agrees that under the current language 100 percent coverage is not required. Texas RE recommends, however, the language clarify and add threshold of acceptable monitoring so the standards applied and enforced consistently. Rather than mandating a specific minimum percentage, Texas RE suggests certain systems, such as operator consoles that are used to operate the Bulk Electric System, should be a mandatory inclusion within the INSM program. Alternatively, the SDT may wish to require entities to justify the parameters they have developed to meet the requirement to "[i]dentify network data collection locations and methods that provide visibility of network communications" so that the rationale for inclusion/exclusion is transparent.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable. See additional comments for more details.	
Likes 0	
Dislikes 0	
Response	

5. The Project 2023-03 SDT held extensive conversations about the term "baseline" and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT's use of the term "network communications 'baseline'" is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The term baseline is appropriate because the entity is creating a baseline of the network activity, although there is room to improve the requirement. Consider rephrasing R6.3 to something like "Evaluate and create a network communications baseline using the collected data in Part 6.2." This should adequately differentiate this baseline from the one used in the CIP-010 standard.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The undefined term "baseline" is ambiguous, and is already in use in CIP-010 in a different context. Suggest revise to define what is meant by "baseline" in this context, preferably use a different term.

Identify clear retention requirements that are achievable with current marketplace offerings. For example, ISPs will leverage netflow data to maintain long term trends on interface and protocol utilization. It's relatively low cost, and low storage requirements, yet allows for historical analysis and trending over time.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No

Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Suggested change: “network communication baseline” to “protocol baseline”. This aligns with the various ICS and non-ICS data communication protocols that could be detected in the network environment.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Wording of 6.3, in particular, needs to be addressed by changing the word “Document” to “Establish” or “Develop” the expected network communication baseline. This will give the Responsible Entity the flexibility in their evaluation of the collected data in how they determine an expected network communication baseline.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

The use of “baseline”, while understandable, will still create overloading of the word as it’s already extensively used in CIP-010 and, by implicit reference, CIP-007 R1 and R2. Suggest the following language for Requirements:
Record, evaluate and pattern the collected data sufficiently such that significant deviations from historical records are detectable.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated.

This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management.

The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic. This change supports the use of vendor proprietary technology for network traffic baselines, where the product may not be able to “output” a baseline but uses trending and comparisons to detect anomalies.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes this requirement will be difficult to fulfill, as we don’t know what a network communication “baseline” will look like. How do we document a baseline? It is also not sustainable to maintain a static documented baseline. PG&E believes this will most likely be defined by the security vendor	

that is being used and probably will not be publicly available (and will probably be internal configuration settings rather than a written baseline). PG&E also believes this requirement may not be feasible or necessary, given the logging and analysis requirements in other R6 sections.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	No
Document Name	
Comment	
Black Hills Corporation does not support the Requirement 6, 6.3 as currently written. Black Hills Corporation agrees with the comment provided by EEI, "EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** (*remove "Evaluate the collected data to document the expected"*) network communication baseline **through methods that record normal traffic to network assets and are continuously updated**."	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
The term baseline can and will be confusing – since CIP-010 use the term "baseline", There should be a different term to be used instead of using the term "network communications baseline". The term 'baseline' already being widely used and understood across industry to refer to a software baseline in CIP-010 R1. Baseline is not sufficiently defined, and many would interpret this to imply a point in time capture of desired system state. The requirement states the baseline should be derived from evaluation of the collected data. However, collected data may differ considerably from the "Expected network communication" as documented in application/OS requirements and could lead to anomalous traffic being included within the baseline. The recommendation would be to specifically define both "network communications baseline" and "software baseline" separately in the NERC glossary of terms.	
Likes 0	

Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	
Comment	

Oncor stands in agreement with comments made by by EEI that states:

"EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a Evaluate the collected data to document the expected network communication baseline **through methods that record normal traffic to network assets and are continuously updated**."

Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State agrees with MRO provided comments:

"The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3 and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish”. The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which is evaluates all network traffic."

Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD recommends that the Standards Drafting Team simply remove the word “baseline” and we propose the following language for Requirement R6 Part 6.3. “Implement methods to evaluate collected data to establish the expected network traffic.”	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
We agree that the concept of a network baseline makes sense but do have concerns that the diversity with which entities might construct these baselines . We support EEI proposed language to include “through methods that record normal traffic to network assets” at the end of 6.3 to encourage alignment on the expected outcome. It may be necessary to specify minimum elements for collection.If the term baseline is problematic, it could be removed all together in 6.3 if adequately specificity is given.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI comments: " EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a Evaluate the collected data to document the expected** network communication baseline **through methods that record normal traffic to network assets**. "	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	

Propose changing the term “document” to “establish." to enable demonstration that a baseline has been established, but not require documentation. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	No
Document Name	

Comment

It would be helpful to have particular aspects of a network communication baseline be clearly defined in the standard (similar to a baseline in CIP-010 R1.1). Maybe some wording like “including but not limited to”, so that utilities have some network communication baseline structure to work off of as recommended by NERC. This would clarify the compliance expectation when providing evidence for network communication baseline.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

If the term “network communications baseline” is to remain undefined by NERC, then the requirement should include language directing the entity to define what constitutes the “expected network communication baseline” that is being documented and monitored. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. This ensures that monitoring and evaluation of deviations is occurring against a well-defined standard, and reduces compliance evaluation ambiguity for the entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP does not agree with the SDT's use of the term "network communications baseline" in Part 6.3. With the industry-approved, virtualization-related changes from NERC Project 2016-02 including the removal of the term "baseline" from the currently enforceable version of CIP-010, the term "baseline" is not anticipated to be used in the future enforceable NERC CIP requirements. In addition, the SDT should consider adding "application flows" as part of the requirement language to help this requirement its overall intent.

SPP proposes the following language for Part 6.3: *Evaluate the collected data to document the expected application flows and network communications.*

SPP also supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	
Response	

David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)

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 RSC	
Answer	No
Document Name	
Comment	

It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline.

The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as "Network Communication Baseline," to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated.

This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management.

The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

"See comments submitted by the Edison Electric Institute"

Likes 0	
Dislikes 0	

Response

Whitney Wallace - Calpine Corporation - 5

Answer	No
Document Name	

Comment

There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)

Likes 0	
Dislikes 0	

Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline.

The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated.

This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management.

The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.

Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

Ameren would like more clarification around the term "baseline."

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	

Comment
Avista agrees with EEI's comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a Evaluate the collected data to document the expected** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer	No
Document Name	

Comment
From the NERC meeting which took place on 1/3/2024, the concept of a baseline was clarified to not be a point-in-time list, a spreadsheet, etc. but more of an expected network communication *behavior* and *functionality* against which the collected data can be evaluated. If this is the case, the Requirement should not have a term (baseline) that is to be interpreted. The focus is on evaluating expected network behavior against anomalous activities. Proposed language: "Evaluate the collected data to maintain the expected network behavior."

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 Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a network communication baseline **through methods that record normal traffic to network assets**.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI's comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	

Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The term "Network communication 'baseline'" lacks clarity and introduces significant potential for confusion, particularly given its distinct usage in CIP-010. Consequently, it is advisable to refrain from employing "baseline" in the context of CIP-007 to avoid misinterpretation. The proposed Measures incorporate the term "expected network communications," which we believe adequately characterizes the information sought. However, the Measure itself falls short in delineating the specifics of the anticipated evidence. A record encompassing "expected network communications" is likely to amass a volume that surpasses human readability. This raises the pertinent question: What elements are anticipated to be included in this record? Does it necessitate an exhaustive enumeration of every conceivable endpoint and each individual protocol? Clarification is essential for a comprehensive understanding of the proposed Measure.	
Likes 0	
Dislikes 0	
Response	

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
More information is needed to determine what would be a suitable baseline. Does an entity have to provide documentation from vendors to support the baseline? Without more information on what constitutes a baseline and what evidence is required to justify the baseline it leaves too much open to interpretation by an auditor. Entities will vary on the methodology used to determine their baselines and this makes it hard for an auditor.	
Likes 0	
Dislikes 0	

Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. CEHE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. CEHE recommends revising the requirement to include a frequent evaluation of entities network communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.	
Likes 0	
Dislikes 0	

Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company does not agree with R6 Part 6.3 as currently written. These requirement parts (6.2-6.5) are detailing a procedural “how” of meeting a security objective, which could be combined into “implement a process to monitor the identified collection points for anomalous activity including connections, devices, or communications” with response criteria and processes. A baseline can be a stated measure of how the entity determines anomalous activity. Southern Company suggests making the standard more future-proof, it needs to be more objective as security principles such as Zero Trust are incorporated with increasingly more communications in device to device encrypted tunnels thus reducing the usefulness of "on the wire" monitoring over time. Virtualization, containerization, micro-segmentation, etc. are all variables in how, and at what level, security monitoring may be best performed in the timeframe of this standard's implementation plan. Currently the language requires the baseline be built only from monitoring the network. We suggest the standard require what the entity is to accomplish, not procedural steps of how to “do” INSM with today’s tools. That is better left to Implementation Guidance or Technical Rationale and could simplify this requirement from its current 7 step process.	
Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. SIGE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. SIGE recommends revising the requirement to include a frequent evaluation of entities network communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Considering the 2016-02 SDT CIP-010 R1 language has moved away from documenting baselines and leveraging automation, the 2023-03 SDT should adopt a similar approach from - 'Evaluate the collected data to document the expected network communication baseline.' To - 'Evaluate the collected data to establish the expected network communications.'	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
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 comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST sees no problem with distinguishing network traffic baselines from endpoint device configuration baselines. We also note that if the most recent modifications to CIP-010 made by the Project 2016-02 SDT are approved by the NERC Board and by FERC, Responsible Entities will no longer be required to maintain configuration baselines as evidence of compliance with that Standard, which will further reduce the risk of confusion.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	

Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the use of the term “network communications baseline” in Requirement R6, sub-requirement 6.3.	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - 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	
Wendy Kalidass - U.S. Bureau of Reclamation - 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), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
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 network communications baseline is clear in Requirement R6 Part 6.3. If the SDT wishes to avoid the use of the word ‘baseline’ in this requirement Texas RE proposes any of the following requirement language alternatives:

- Evaluate the collected data to document the expected network communications profile.
- Evaluate the collected data to document the expected network communications traffic.

• Evaluate the collected data to document the expected network communications traffic pattern(s).	
Likes 0	
Dislikes 0	
Response	

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term “anomalous.” The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of “anomalous” was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term “anomalous” was the appropriate term to use to describe that methodology. Do you agree that that the term “anomalous” effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments filed by the IRC SRC and adopts them as its own.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We understand the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Anomalous traffic may be expected from the baseline during outage or troubleshooting or testing, and it may be impossible to capture them in the network baseline. The standard should have verbiage to exclude those scenarios.	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	No
Document Name	
Comment	
AZPS believes that "anomalous activity" is ambiguous. We recommend language similar to the question above "deviations from a normal network communications baseline"	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	
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 RSC	
Answer	No
Document Name	
Comment	

Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The term "anomalous," is too vague and covers too many potential activities. The SRC recommends using the phrase from FERC Order No. 887: "anomalous network activity indicative of an attack in progress" as detailed below: *CIP-007-X Table R6 – INSM: Part 6.4 Requirements* *Deploy one or more method(s) to detect anomalous **network** activities **indicative of an attack in progress**, including connections, devices, and network communications using data from Part 6.2.*	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
While SPP does not have concern with the term "anomalous", SPP believes the current purposed language is beyond the scope of FERC Order 887, which states "anomalous network activity indicative of an attack in progress." SPP proposes updating the language in Parts 6.1, 6.4, 6.5, and 6.6 to include the language "anomalous network activity indicative of an attack in progress."	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	

James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to E-ISAC in CIP-008, they should be afforded that opportunity for anomalous events in this standard. This also reduces compliance evaluation ambiguity for the entities both internally and externally.	
Likes 0	
Dislikes 0	
Response	

Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.	
Likes 0	
Dislikes 0	

Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends where possible align proposed terms with NIST current definitions. NIST definition examples: Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences. Behavioral Anomaly Detection - A mechanism providing a multifaceted approach to detecting cybersecurity attacks.	
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	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

While Dominion Energy understands why the term "anomalous" was chosen by the SDT, we recommend additional clarifying language be added to make it clear that stakeholders, who have the best understading of their networks, are responsible for determing what is anomalous. We recommend the addition of the phrase "as determind by the Registered Entity" be added to qualify anamolous.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State recoomends using the words normal or abnormal in place of anomalous.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

The recommendation would be not to use the word “anomalous” at all. Recommend the use of “unusual communications that need to be investigated” instead. Using the terms “unusual communications that need to be investigated” removes the ambiguity of what an entity would define as “anomalous”.

If the word “anomalous” is used in the standard, it must be defined in the glossary of terms with the definition specific to the SDT’s intent of its definition, namely, “unusual communications that need to be investigated” since the dictionary definition of the word anomalous is, “deviating from what is standard, normal, or expected.”

This definition would allow for entities to consider an “unusual communications that need to be investigated” event as “normal” or “expected” and the expected understanding of the word anomalous in this context and requirement would be lost.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The term “anomalous” is too broad. We suggest focusing on wording similar to “deviations from the network communications baseline.”	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
SDT should consider defining anomalous to avoid any confusion for entities. See additional comments for more details.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes the term “anomalous” is vague. PG&E recommends using the phrasing from FERC Order 887 “anomalous network activity indicative of an attack in progress.”	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Manitoba Hydro understands the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance. This clearly defines the scope of the standard, for example if a product detects anomalies related to system network communication malfunctions these may be useful to an entity but out of scope of compliance. Leaving the term “anomalous” in continues to differentiate between detected “anomalous” activity and a confirmed attack in progress.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

The use of “anomalous” is fine however suggest including “potentially” and to align with proposed language from proposed R6P2:
Deploy one or more method(s) to detect potentially anomalous activities, including connections, devices, and network communications using data from Part 6.2

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

MRO NSRF understands the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The undefined term “anomalous” is ambiguous and may create confusion for both entities and the CEA to determine what specific activities are included. Suggest revise to provide a clear criteria for determining what activities are “anomalous” that is consistent with existing CIP-008 obligations.	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
The term “anomalous” is not specific enough. It would be clearer to build on the language used in R6.3. In R6.3, we essentially determine what is not “anomalous” (e.g., what is acceptably part of the network communications baseline). Consider rephrasing as “to detect activity that deviate from the network communications baseline identified in Part 6.2” or similar. This clarifies the intent, eliminates the need to include “anomalous”, enhances cybersecurity by converting the “black list” to a “white list” monitoring method, and reinforces the importance of the communications baseline throughout R6.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	

Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	

Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	

Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
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 is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with use of the term “anomalous”.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
One potential issue NST does see here arises from the SDT's assertion, in the draft Technical Rationale document, that a baseline is "Continuously updated by a computer" and not a "Point-in-time list." We believe these assertions are incorrect. Merriam-Webster's online dictionary defines "baseline" as, "a usually initial set of critical observations or data used for comparison or a control." Similarly, several references NST consulted define network baselines as "snapshots" that can be used to set expectations about traffic types, volumes, sending and receiving devices, etc. during some period of time (e.g., weekdays from 8 AM to 6 PM local time). While we certainly agree baselines	

should be updated periodically, we are hard-pressed to understand how anomalous traffic can be detected if a baseline that is intended to represent "expected" traffic is being ***continuously*** updated.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI is of the opinion that the term "anomalous" is sufficiently clear to describe the methodologies. "	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the term "anomalous" is appropriate.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
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	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 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), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
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	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 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	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

It would be clearer to use language in R6.5 like that of CIP-005-7 R1.5 "Have one or more methods". Also, as stated in question 6, not using the term "anomalous" would be beneficial here. Consider language like "Have one or more method(s) to evaluate activity that deviates from the baseline identified in Part 6.2." This approach supports the ability to evaluate the finding before initiating a CIP-008 Cyber Security Incident determination while maintaining continuity with other existing standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The undefined term "anomalous" lacks the clarity to distinguish between activities addressed in Part 6.4 and activities that should initiate a CIP-008 process.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

As above, suggest the inclusion of "potentially" and to outline that anomalous may not be malicious:
One or more process(es) to evaluate potentially anomalous activity identified in Part 6.4 to determine appropriate action including, but not limited to, adjustments to the traffic patterns from Part 6.2 or investigation as a potential security incident.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	
Comment	

It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.

There is no wording stating specifically that escalation and potential initiation of a responsible entity's CIP-008 process is the appropriate action if a legitimate threat is detected.

Likes 0	
Dislikes 0	
Response	

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	
Comment	

It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. To clarify the link the requirement could be re-worded:

One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine if it is related to a Cyber Security Incident.

The measures lists potential evidence as "documentation of responses to detected anomalies". Manitoba Hydro suggests removing this from the measures to focus on evidence related to having the process documented. When systems are first put in they may generate a lot of alerts before they are "tuned" and evidence of review of every single alert may be burdensome without any practical security value.

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	

AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE recommends the following requirement language: One or more process(es) to evaluate anomalous activity identified in Part 6.4 as a potential Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
It is not clear how to determine when action is required.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	

Comment
I believe this question may refer to an older version of the draft standard. This question makes more sense regarding Part 6.5, and the INSM drafting team outreach presentation discusses CIP-008 in the context of Part 6.5. However, the actual language of Part 6.5 does not reference CIP-008, and therefore any anomalous activity could be interpreted as an attempt to compromise and/or an actual compromise that triggers the requirements of CIP-008. It isn't enough to include the SDT's intention in an outreach presentation - if it isn't in the standard, an auditor will not consider it.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment
This question appears to reference CIP-007-X Requirement R6 Part6.5 and this question is not clear and not very well defined. We recommend changing Requirement R6 Part 6.5 to state: “Implement methods to evaluate anomalous activity identified in Part 6.4.”

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	

Comment
In 6.5 Duke Energy recommends additional language to clarify the intent of the evaluation. *One or more process(es) to evaluate anomalous activity identified in Part 6.4 for indications of an attack in progress, and if such indications are detected, to determine appropriate action.*

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	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As currently written, neither R6 nor any of its parts say anything about CIP-008. NST suggests language such as, "Develop and deploy methods to detect anomalous network activity and to identify potential Cyber Security Incidents."	
Likes 0	
Dislikes 0	

Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends adding additional language to CIP-007 R6 to clarify that this occurs before the determination of a Cyber Security Incident.	
Likes 0	
Dislikes 0	

Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Suggest including language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vise versa.	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The language wasn't that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	

Since the requirement language in R6 Part 6.5 does not mention CIP-008 or Cyber Security Incidents, there is no relationship established between R6 Part 6.5 and CIP-008 or a Cyber Security Incident. Additionally, the requirement language may fall within the current processes identified for Cyber Security Incident Response by the Responsible Entity, and could cause multiple response paths to be created.

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 RSC

Answer	No
Document Name	

Comment

The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to “identified”.

It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.

There is no wording stating specifically that escalation and potential initiation of a responsible entity’s CIP-008 process is the appropriate action if a legitimate threat is detected.

Likes 0	
Dislikes 0	

Response

Whitney Wallace - Calpine Corporation - 5

Answer	No
Document Name	

Comment

The language wasn’t that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to “identified”.

It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.

There is no wording stating specifically that escalation and potential initiation of a responsible entity’s CIP-008 process is the appropriate action if a legitimate threat is detected.

Likes 0	
Dislikes 0	
Response	

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.

Likes 0	
Dislikes 0	
Response	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
As written, the requirement could potentially result in a self-report if any “anomalous activity” occurs and is not detected.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The use of the term "anomalous' in Requirement R6, Part 6.4 is fine, but this starts to overlap with an entity's CIP-008 Incident Response Program". An entity already has definitions for attempt to compromise in the Incident Response Plan and if "anomalous" activity is detected it should refer back to its incident response plan. Just because an entity detects anomalous activity and they refer to their incident response plan it does not mean it is a Cyber Security Incident, it just needs to be investigated.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not believe that Requirement R6, Part 6.4 nor Requirement R6, Part 6.5 addresses the process of evaluating anomalous activity prior to escalation and potential initiation of a responsible entity's CIP-008 process. Requirement R6, Part 6.4 requires methods to detect anomalous activity. Requirement R6, Part 6.4 does not address investigation or evaluation. Requirement R6, Part 6.5 requires a process to evaluate the anomalous activity identified in Requirement R6, Part 6.4. SIGE suggests including "prior to the initiation of a responsible entity's CIP-008 process" in Part 6.5 so that the new requirement would read, "One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action, prior to the initiation of a responsible entity's CIP-008 process."	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.	
Likes 0	
Dislikes 0	
Response	

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests that clear language be added to tie R6.5 and/or R6.6 to CIP-008 in coordination with the Project 2022-05 drafting team. How a hand-off from a suspected malicious event is directed into a reporting requirement for “attempts to compromise” is under discussion under Project 2022-05. Ambiguity around analyzing whether an event is a security incident, what threshold for reporting such an incident might need, and the process to tie it into incident response activities including mitigation has the potential for creating duplicative and distracting requirements. BPA recommends the SDT change the word “Deploy” to “Utilize”. BPA believes deployment implies implementation of new technologies not currently in the Registered Entity’s environment.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 DT was clear that Part 6.4 would occur before determining if a Cyber Security Incident had occurred.	

Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear."	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	

Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
SPP agrees that the process to determine appropriate action regarding anomalous activity in Part 6.4 occurs prior to escalation and potential initiation of a Responsible Entity's CIP-008 process (i.e., before the determination of a Cyber Security Incident). However, there appears to be a typographical error in this question. SPP believes the SDT intended to reference Part 6.5 since it is more appropriate for the content of this question.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes

Document Name	
Comment	
The NAGF believes that the process has been adequately clarified.	
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 language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The process is clear as laid out in 6.4 detection and 6.5 evaluation. It is only this question that is confusing, referencing only 6.4 in a discussion about the 6.5 evaluation.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes

Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes

Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
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	
Byron Booker - Oncor Electric Delivery - 1	
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	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - 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	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
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	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
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	

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes outlined in Question #5 (above).

Likes 0	
Dislikes 0	

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CEHE believes that the requirement itself is objective- based; however, the scope described in the CIP-007-X Technical Rationale is in broad prescriptive terms. The Technical Rationale should clearly state that it does not determine the scope.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

There doesn’t appear to be much latitude in how to implement methodology.

Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC believes requirement part 6.3, which mandates the evaluation of collected data to document the expected network communication baseline, poses a limitation on certain technology platforms, notably Intrusion Detection Systems (IDS). This constraint arises from the inherent characteristics of certain IDS technologies, which may not facilitate the documentation of an expected network communication baseline. In specific instances, certain IDS technologies generate alerts predicated on Indicators of Compromise (IoC) signatures without establishing a network model for triggering alerts based on anomalous behavior against the established network communication model.

The FERC order specifically identifies IDS as a potential technology for implementing Internal Network Security Monitoring.

In Part 6.1, GSOC recommends aligning the use of terms like "Cyber Asset" in Requirement language with the terminology used in the recently approved versions of the Standard drafted by Project 2016-02. Specifically, in that version of the Standard, the coverage would only extend to a physical Cyber Asset, overlooking a Virtual Cyber Asset.

In Part 6.1, the exclusion labeled "(excluding serial)" lacks clarity, especially when contemplating the utilization of serial-based network communications like T1's. GSOC suggests refining this exemption to enhance clarity, citing other instances in the Standards where exclusions for this type of communication are present or possibly utilizing routable communications.

In Part 6.2, GSOC finds it unclear what type of log data is required and the necessary retention policy to comply with the current wording. GSOC proposes incorporating objective language that allows entities to define an appropriate retention period for the log data.

Concerning Part 6.3, GSOC notes that the Requirement lacks sufficient clarity regarding what constitutes an evaluation. It merely states that the entity should look for deviations from expected network communications without specifying what should be included in expected communications.

GSOC suggests that Part 6.4 could potentially be combined with 6.3, and perhaps even 6.5, for enhanced clarity.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Although R6.4 allows the latitude for various INSM Methodologies and technologies; it also must satisfy R6.1. Hence, R6.1 should be defined in more detail. See response to Q4 above.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
There doesn't appear to be much latitude in how to implement methodology.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	

Comment
Tacoma Power does not agree that the Table R6 requirements allow latitude for various INSM methodologies. The NSM process described in R6 is one way to solve the Internal Network Security Monitoring Order, but other methodologies exist to gather and alert on malicious internal East/West traffic. It may be beneficial to recast the entirety of R6 in the Risk Mitigation ideal to mitigate the risk posed by malicious network activity within the CIP-Networked Environment. Part 6.2 should include “per system capability” to ensure that entities are not required to collect data on systems that may not have the capability.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	

Comment
SPP does not agree the SDT was successful in creating an objective-based approach, particularly with the concerns expressed in SPP’s comments for questions 4, 5, 6, 9, and 11.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	

Comment
Duke Energy greatly appreciates the work of the drafting team to create INSM requirements while trying to balance the need for flexible language. We are concerned that that the draft requirement allows too much latitude and will result in significant differences between INSM programs from responsible entity to responsible entity.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
Based on the technical rational and the various diagrams that have been presented, SMUD believes that the INSM requirements are both prescriptive and subjective.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
A 'No' response is based on ambiguities but agree that latitude is allowed for various INSM methodologies and technologies to be used now and in the future.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes some of the requirements need additional clarification, as noted in our earlier comments.	

Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not find that R6 Part 1 is objective or will lead to objective outcomes. Please see comments above.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Consider leveraging the OSI model to clearly identify the target depth of monitoring and retention. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	

Comment
We agree that Requirement R6, as written, provides latitude for various methodologies and technologies to be used. However, the broadness and ambiguity of some of the requirements and measures may lead to disagreements between entities and auditors that sufficient monitoring and documentation have been provided. Without providing more specific guidance on the type of information that should be available within data logs, retention periods, response timelines, and assessments of anomalous activities, this could lead to auditors issuing PNCs for an entity where they deem that the documentation being provided as evidence is insufficient.

Likes 0	
Dislikes 0	

Response

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment
Project 2023-03 SDT did create a requirement that was objective based and allowed latitude for various INSM methodologies, but this is a double-edged sword, with the large amount of latitude it leaves too much varying interpretations between what an auditor is expecting, and an entity is doing. In addition, there will be varying ways in which entities across different regions meet this requirement some will go above and beyond while others do the bare minimum which again leaves it up to an auditor if enough is being done to be compliant.

Likes 0	
Dislikes 0	

Response

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	Yes
Document Name	

Comment
See comments submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
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 language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above.	
Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted 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 RSC	
Answer	Yes
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who	

use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF believes that the proposed Requirement R6 is objective based and will allow for various INSM methodologies and technologies.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	

Comment	
This effort and work to meet the requirements and allow flexibility in execution of the requirements is greatly appreciated.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above."	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees the language in Requirement R6 is objective and allows latitude, noting our proposed changes above.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	

Answer	Yes
Document Name	
Comment	
Manitoba Hydro appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
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	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
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	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
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	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
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	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
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	
Byron Booker - Oncor Electric Delivery - 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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

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

Answer	No
Document Name	

Comment

The ambiguity with the proposed language makes it difficult to assess implementation timeframes.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

MRO NSRF appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.

Likes 0	
Dislikes 0	

Response

Karen Artola - CPS Energy - 1,3,5 - Texas RE

Answer	No

Document Name	
Comment	
With the increased concern of critical infrastructure infiltration by foreign adversaries, 36 months should be applied to all systems inside and outside of Control Centers. This should be conceivable since Part 6.1 provides latitude to not having 100% coverage of network data collection locations.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
36 months for Control Centers and 60 months for applicable systems located outside Control Centers should be sufficient only if the language in Part 6.1 of "100 percent coverage is not required" is updated with the following (or similar): "*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.*"	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Without clear expectations of the Drafting Team toward the Industry Members, we cannot support the implementation Plan of CIP-007-x.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In March 2022, BPA made the following comment in response to FERC's INSM NOPR: *"Bonneville estimates implementation timelines for INSM on High Impact BES Cyber Systems alone to be around three to five years. If entities are also required to adopt INSM on Medium Impact BES Cyber Systems with ERC, it would likely take on the longer end of that timeline to implement.* After reviewing the new requirement language in R6, BPA believes more time will be required to implement an INSM program. This takes into consideration the effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Manitoba Hydro appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. The 36 month timeline may or may not be sufficient depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to	

Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy has concern over the 36 month implementation due to supply chain concerns. Dominion Energy requestis 48 months for Control Center and keep 60 months for the other applicable systems not located at Control Centers.

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

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree with the proposed schedule.	
Likes 0	
Dislikes 0	
Response	

Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Unknown if 36 months is sufficient for implementation - it depends on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. Further, the Technical Rationale on pg. 4 should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
There could be cases where entities may not be able to procure, test, configure, and fully deploy an INSM solution within the stated months. A suggestion is to allow each entity to respond with an appropriate timeframe for implementation that is viable to it. The Regional Entity can be afforded oversight to their entities’ commitment.	

Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP does not agree with the Implementation Plan for Draft 1 of proposed CIP-007-X based on the concerns expressed in SPP's comments for questions 4, 5, 6, 9, and 11.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.

Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

If the FERC Order involves monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC finds the provided timeframe sufficient. Nevertheless, due to the ongoing lack of clarity in the scope, it is challenging for us to provide comments, resulting in a “No” response to this question.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in order to ensure communications is not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We appreciate the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to Q4 this should be removed and replaced by continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity." If Part 6.1 governs, 36 months should be sufficient. The problem is with the Technical Rationale regarding Vendor Support on p. 4: "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity	

to support cybersecurity collection systems such as INSM or endpoint logging agents." This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 implementation plan.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation supports the proposed Implementation Plan, but 36 months would be the minimum time required to implement. Black Hills Corporation also agrees with the proposed changes from EEI, “EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

(remove "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.")

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.”

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Constellation has no additional comments.

Kimberly Turco on behalf on Constellation segements 5 and 6

Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

Oncor stands in agreement with comments presented by EEI that states:

"EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging."

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports the proposed Implementation Plan and the phased approach.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI comments: " EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern

equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents. Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging. “	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes

Document Name	
Comment	
The NAGF supports the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
The implementation plan could clarify these timelines better and how they stack. Currently it is not obvious.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment

Avista agrees with EEI's comments and recommendation for Technical Rationale:

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Remove the following:

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment

capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Insert the Following:

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with EEI’s comments and recommendation for Technical Rationale:	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	

Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
3 years for Control Centers and 5 years for non-control centers is acceptable but more technical guidance or requirement clarity is required to meet auditors' expectations. The technical rational and guidance need more clarity to align the auditors and implementors.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Yes, however the more time the better some entities will already have upgrades planned and this will have to be figured into the upgrades.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	

Southern Company agrees with the implementation duration. However, Southern Company would offer the suggestion to have separate sentences with "…the standard shall become effective for Control Centers on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees". "…the standard shall become effective for medium impact BES Cyber Systems with ERC not located at Control Centers on the first day of the first calendar quarter that is sixty (60) months after the date the standard is adopted by the NERC Board of Trustees".

We believe this would help with confusion that is occurring with the Implementation Plan as currently written.

Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3

Answer	Yes
Document Name	
Comment	

Exelon is responding in support of the comments provided by EEI.

Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
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	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
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	

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

Developing and maintaining the necessary processes and procedures to maintain a sufficient level of documentation for compliance purposes will create a need for entities to increase the number of FTEs. We have already seen an increase in costs associated with INSM from vendors over that past few years and expect that once this requirement is approved, costs will increase further due to the limited number of vendors with applicable OT solutions.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	
Comment	
No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It will take an untold number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	
Comment	
It is Southern Company's opinion that the cost effectiveness of the current proposed requirements can vary greatly depending on what percentage below 100% in R6.1 is determined to be compliant in each region, and what specific Cyber Assets are determined to require monitoring. In addition, there are significant concerns about supply chain constraints given a limited pool of Operational Technology (OT) vendors with INSM products.	
Likes 0	
Dislikes 0	
Response	

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	No
Document Name	
Comment	
Cost effectiveness is difficult to judge with the first draft. Ultimately cost effectiveness will be determined by the final draft. Additional oversite and help may be required for compliance.	
Likes 0	
Dislikes 0	

Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
If the scope of the FERC Order requires monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC contends that cost-effective solutions can achieve this goal. However, there is ambiguity in interpreting how to manage EACMS and PACS INSM data. In instances where these Cyber Assets might exist outside the ESP, it becomes unclear how much equipment would be necessary to retrofit existing infrastructures.	
Likes 0	

Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The new requirement is inherently not cost effective.	
Likes 0	

Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	
Likes 0	

Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	
Tacoma Power needs additional clarity to understand the scope of work and boundaries of what's covered in this Standard in order to assess cost.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	

Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks the SDT to consider the potential cost that may arise from the scope of this requirement. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, and storing of all data between every cyber assets within an ESP, for any length of time, will be substantial. Not all network architectures are created equal and could be more costly and time consuming to implement for some Responsible Entities than others. Virtualization of network, server, and storage infrastructure, and the complexity it brings to the table, has the potentiality to make packet captures, baselining of traffic, monitoring, analyzing, and alerting much more difficult if a Responsible Entity is unable to obtain visibility into all of the network traffic within a subnet.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
It is not clear that all sub parts of requirement R6 could be cost effective. It is a new requirement that would mandate an entity to effectively not only procure a brand new solution, but produce an entirely new process and procedures, in addition to the human resources and associated roles and responsibilities, with which the entity must comply. Although it's possible certain entities would not have a financial burden for this kind of expenditure, it may be a significant burden for others.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No

Document Name	
Comment	
The cost effectiveness is dependent upon updating the langauge to 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount. Further, the Technical Rationale on pg. 4 should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree the proposed changes are cost-effective.	
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	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
This inclusion of cyber assets outside of High BCS and Medium BCS with ERC is not the most cost-effective approach to increasing the security posture of those cyber assets. Addressing boundary-level (north-south) controls for these assets would be more cost-effective approach and a logical first step to creating a common understanding of a “trust zone” for these device types before an east-west monitoring construct is applied.	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD feels that the determination of cost effectiveness varies based on the methodology used, but prescribing network communication baselines as the methodology would not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
NIPSCO has not determined whether R6 will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	

Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
The expansion of the scope of the FERC Order to include PCA, EACMS, and PACS will significantly increase the implementation costs. Although the standards drafting team indicated that assets not currently in scope of the CIP standards are not included (for example, Corporate AD servers that are not currently EACMS), it is likely that audit teams will have different interpretations.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Not too sure what the exact cost will be for each entity, but the cost of monitoring can be a costly endeavor for many entities, including SRP.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	

PG&E cannot determine if the modifications are cost effective at this time. There are still unknowns as to the required scope (% coverage) and data retention requirements. We would like to see more industry feedback before deciding.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	

Comment

May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This change in the standard will result in significant resource expenditure, including wholesale replacement/architecture of existing networks, that will be exceptionally costly and such costs will be passed on. Implementing this standard will result in the potential of hundreds of network devices all requiring replacement with devices that are significantly more costly simply to add the ability to execute some form of intra-lan monitoring. Additionally, the potential reliability impact of requiring major network architecture needed is much higher than modest security gains.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	

Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Depending on if the language in Part 6.1 is updated, this may or may not be cost effective. If the language of "100 percent coverage is not required" is updated with language similar to the following: "*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.*", then the implementation plan should be sufficient as proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
May or may not be cost effective depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to Q4 this should be removed and replaced by continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity." If Part 6.1 governs costs could be contained to a reasonable amount. The problem is with the Technical Rationale regarding Vendor Support on p. 4: "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents." This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware may not be cost effective.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The ambiguity with the proposed language makes it difficult to assess implementation cost.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree and disagree. Since the standard allows the latitude, cost effective solutions can be implemented but will it be good enough to meet the auditor's expectations? The technical rational and guidance need more clarity to align auditors and implementors.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	

Answer	Yes
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives	
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 RSC	
Answer	Yes
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
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	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
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	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	

Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	

NA	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	
Document Name	
Comment	
Oncor will not submit comments on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.	
Likes 0	
Dislikes 0	
Response	

11. Please provide any additional comments for the SDT to consider, if desired.

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

Answer	
Document Name	

Comment

Data retention requirements are ambiguous and subject to interpretation by entities and the CEA. Suggest revise to provide guidance regarding retention requirements by data type.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	
Document Name	

Comment

MRO NSRF appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Regarding CIP-008, MRO NSRF urges the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point.

Lastly, MRO NSRF thanks the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.

Likes 0	
Dislikes 0	

Response

Karen Artola - CPS Energy - 1,3,5 - Texas RE

Answer	
Document Name	

Comment

For Part 6.5, reword sentence to begin, “Develop one or more process(es)…”

For Part 6.7, reword sentence to begin, “Develop one or more process(es)…”

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	

Answer	
Document Name	

Comment

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA recommends adding language addressing the intended periodicity or ongoing nature of the proposed R6 Parts. BPA can’t determine based on the proposed requirement language how often the ERO-Enterprise (ERO-E) would expect entities to perform the location identification, data logging, and baselining requirements. In order to avoid inconsistent interpretations among Registered Entities and auditors across the ERO-E, BPA recommends the SDT include language in the requirements that specifies a minimum cadence by which the aforementioned tasks should be completed or that clarifies the RE is empowered to determine the cadence. The SDT should clarify if the intent is to have methods and processes for R6.4 through R6.6 that address patterns of behavior and processes to analyze them, rather than isolated pieces of traffic.

BPA also recommends adding minimum log retention timeframes as a compliance metric and to align with other CIP standards. R6.7 should be modified to cover risk of data exploitation as follows: “…protect the data collected in Part 6.2 to mitigate the risks of exploitation, deletion, or modification by an adversary…”

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	
Document Name	

Comment

Manitoba Hydro appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	

Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 appreciates the effort the DT had taken in creating a Standard to meet FERCs Order with a very aggressive time frame. PG&E will be waiting to see the next version of these requirements based on our and other Registered Entities feedback that include the scope and percentage of coverage of Cyber Assets.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	
Document Name	

Comment

Section 4 comment: The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable to 6.1. The entity should also consider documenting the reasons why others were not considered critical.

Stating "100 percent coverage is not required" can lead the entities to only monitor a few CIP network interfaces without any clear direction to comply with the standard, and not use this opportunity for the intent purpose of the standard to monitor and protect the internal networks from security threats.

Section 6 comment: Per the information gathered from CIP-007-X, the use of word “anomalous” doesn’t clearly indicate the use of both network baseline and the signature-based tools to identify anomalous. E.g., 6.4 states “Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2” which could lead entities to use only log collected data and not network baselines indicated in 6.3 to detect anomalous (including malicious) activities.

Additionally, SDT should consider defining anomalous to avoid any confusion for entities.

Additional Comment

There is no requirement to reevaluate the environment after changes or on a periodic basis to ensure that the entity is monitoring the higher risk traffic.

Likes 0	

Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	
Document Name	

Comment

Constellation has no additional comments.

Kimberly Turco on behalf on Constellation segements 5 and 6

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

It appears by the name of the R6 table, Internal Network Security Monitoring, the intent of this requirement is to monitor internal network traffic. However, this intent is not present in the requirement language.

For example, Requirement R6 Part 6.1 states that communications between applicable Cyber Assets are in scope. High impact BCS are in scope, as are medium impact BCS with External Routable Connectivity. These BCS are commonly found in discrete networks, however the requirement language does not clearly exclude from scope communications between these applicable systems found in discrete networks.

If the SDT intends for communications between Applicable Systems in discrete networks to be in scope, then no change is needed. If the SDT does not intend for communications between Applicable Systems in discrete networks to be in scope, Texas RE recommends modifying the requirement language to convey this.

Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	
Document Name	
Comment	

Oncor stands in agreement withg the comments being submitted by EEI that states:

"BCSI Implications (NEW Proposed)

For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

(NEW Proposed) EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. Suggest either deleting this phrase or changing it to “detecting attacks that may bypass electronic security perimeters”.

EEI suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.

(**NEW Proposed**) EEI additionally suggests the following boldface edits (below) for Requirement 6, part 6.5 to make it clearer the expectation that entities have when they are evaluating anomalous activity.

6.5 One or more process(es) to evaluate anomalous activity identified in Part 6.4 **and to determine appropriate action which include a process for:** **6.5.1: Identifying an attack in progress and actions to be taken in response; and** **6.5.2 Evaluating anomalous activities and actions to be taken in response."**	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	
Document Name	
Comment	
If the scope of this proposed standard was limited to the scope of the FERC Order (assets within the Electronic Security Perimeter), then this standard language should be part of CIP-005, not CIP-007.	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	

Document Name	
Comment	

1. Part 6.5 language is inconsistent with the other R6 sub-parts. All others start with an action verb. We suggest updating 6.5 to begin as "Evaluate anomalous activity...". The process language is inherited from the higher-level R6 requirement language.

2. Part 6.7 - Same statement as for Part 6.5 - We suggest beginning it with "Protect the data collected..."

Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	
Document Name	
Comment	

SMUD appreciates the Standard Drafting Team's effort to revise CIP-007-X to include INSM requirements, but we have the following additional recommendations:

- Move Requirement R6 Part 6.4 (deploy) so that it is before Part 6.2 (log). Part 6.4 should become Part 6.2, then Part 6.2 will then become 6.3, and Part 6.3 will become Part 6.4 with all other parts staying where they are;

- Move all INSM requirements and parts to CIP-005; and

- In the Applicable Systems column, just state EACMS and/or PACS. Do not add where they perform access control functions. There are no other CIP requirements that state anything other than EACMS and/or PACS.

Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	
Document Name	
Comment	

Duke Energy thanks the Drafting Team for their work to thoughtfully address FERC Order 887. There are some additional items that we would like to recommend to add clarity to the INSM revisions.

- Duke Energy recommends Requirement 6.1 is updated to require entities to specify the types of data to be collected in their documented processes, so that the data that will be expected for part 6.2 is clearly tied back to part 6.1.
- Additionally, use of the same phrase “network data” in 6.1 and 6.2 would bring greater clarity to the requirements, updating 6.2 to read “Log collected network data at the network locations identified in Part 6.1.”
- We also request clarity on the use of the term “connections” in 6.1. Does this intend to refer to TCP/UDP “connections” or the connecting and disconnecting of devices to network switches or some other definition of this term? Alternative language such as “monitor and detect anomalous activity, including the presence of anomalous devices in the network and use of anomalous communication protocols in the network” would provide a clearer requirement.
- Duke Energy also recommends that the INSM requirements are moved to their own Standard outside of CIP-007. CIP-007’s traditional focus on device-level security controls is at odds with the broader subject matter of network monitoring, and following the model used by CIP-012 for a new subject matter with no current analogous scoping would facilitate the introduction of this technology and scope, as well as lay the groundwork for elimination of duplicate requirement language in CIP-007 and CIP-003 if Low applicability later added.

Likes 0	
Dislikes 0	

Response

Joshua London - Eversource Energy - 1, Group Name Eversource

Answer	
Document Name	

Comment

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Similar to above, suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below) Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.	
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	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE agrees with two of EEI additional comments: “EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to “that has bypassed other electronic security controls”. EEI suggested adding “in Part 6.2” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below) Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity. “ **“Data Collection Methods, Pages 9 through 10**	

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.”	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes it would be helpful for R6 Part 6.6 to identify a minimum retention period for INSM data unless the SDT intends for it to be the standard 3-year period defined in Section C Part 1.2 ("Evidence Retention"). The language in the proposed Measure for 6.6, "...with data retention configuration with timelines sufficient to perform the analysis of anomalous activity" is vague and could easily be subject to a considerable number of widely different interpretations.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	
Document Name	
Comment	

In Part 6.2, the measure describes an example evidence, which is the data collected. It is not clear why the focus is on the data collected and not the configuration of logging the data, which is the actual stated requirement.

Observation: CIP-007 R6 applicability assumes all assets are known and classified according to CIP-002 and only requires baselining of network traffic between applicable assets. But if an unknown malicious device is put on the network, because it is unclassified and not a BCA, PCA, EACMS, or PACS, and is on its own interface, the entity does not have to pay attention to it or its anomalies. Example – if someone installs a rogue device on the network that initiates a portscan, the entity does not have to recognize the device or the portscan as a network baseline deviation. Along those lines, because TCAs are excluded from applicability, the entity does not have to pay attention to TCAs even though their insertion on the network at odd hours may be anomalous. The structure allows the entity to entirely ignore rogue devices as an attack vector.

Likes 0	
Dislikes 0	
Response	

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	

SPP would like the SDT to consider the following:

Comment for Part 6.2:

SPP is concerned with the requirement language for Part 6.2. The proposed language is open to interpretation and could significantly impact the cost of storage as well as create compliance risk. What needs to be logged? How should the log be evidenced? Is a summary sufficient? How long do the logs need to be retained?

Comment for Part 6.4:

The proposed language for Part 6.4 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.4:

Using the data collected pursuant to Part 6.2, deploy one or more method(s) to detect anomalous network activity indicative of an attack in progress.

Comment for Part 6.5:

SPP suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

SPP proposes the following language for Part 6.4:

One or more method(s) to evaluate the anomalous network activity indicative of an attack in progress identified in Part 6.4 and determine appropriate action.

Comment for Part 6.6:

The proposed language for Part 6.6 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.6:

One or more method(s) to investigate anomalous network activity indicative of an attack in progress.

Comment for Part 6.7:

SPP does not agree with using the term “adversary” in a NERC requirement due to its ambiguity. SPP also suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	

Comment

The NAGF has no additional comments.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike

Answer	
Document Name	

Comment

TPWR believes that the INSM Requirements fit better in CIP-005, due to the Purpose statement found in the latest CIP-005-8: "To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).", **than in CIP-007 which contains the Purpose** "To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)." The Title of CIP-005 may be due for an update as well, since the Title remains "Electronic Security Perimeter(s)" which is no longer fully inclusive of all that CIP-005 includes. One option for the Title of CIP-005 would simply be "Network Security."

Tacoma Power offers this language for the high level R6:

"Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-XXX-X Table RX – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed network perimeter-based security controls."

Tacoma Power believes that the requirement language provided does not align with the scope of monitoring identified in the Webinar on the slide titled 'Interpretation of the Term "CIP Networked Environment"'. Specifically, many of the red "out-of-scope" network paths are not out of scope based on the requirement language. Specifically between the EACMS/EAP and the EACMS Access Control and the EACSM/Intermediate System. EACMS/EAPs and EACMS/IS both perform access control functions and are therefore specifically included in scope. Additionally there are a significant number of additional "in-scope" network paths that are not clarified on the diagram, since the diagram only includes a single ESP and the current language does not limit the scope to the networks associated to each individual Applicable System.

Editorial Comments on Section 3, Purpose:

- The purpose statement should include the acronym after "BES Cyber Systems", as follows:

"To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems **(BCS)** against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

Editorial Comments on Section 4, Applicability:

- The term "Special Protection System" and "SPS" should be deleted throughout Section 4.
- Regarding Bullet 4.2.3.5: delete "-5.1" from CIP-002-5.1. The bullet should read "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the **CIP-002** identification and categorization processes."
- The following exemption is missing and should be added as Bullet 4.2.3.3: "4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations."
- Bullet 4.3 is missing. Recommend adding this bullet, as follows: "4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies."
- Bullets 4.2.3.1 and 4.2.3.2 should refer to "Cyber Systems" and not "Cyber Assets"

Editorial comments on Table R6:

- In the "Applicable Systems" column, the word "impact" should not be capitalized. Additionally, the acronym "BCS" should be used instead of "BES Cyber System" and "ERC" instead of "External Routable Connectivity." Example of how this should be written: "Medium **impact BCS** with **ERC** and their associated…"

Comments related to alignment with Project 2016-02, CIP Virtualization:

- The title of CIP-007 Table R1 should be changed from "Ports and Services" to "System Hardening" to align with the Project 2016-02 changes. The title of Table R1 should also be changed in the R1 language.
- The title of CIP-007 Table R2 should be changed to "Cyber Security Patch Management" to align with Project 2016-02.

- The language in the following Requirement Tables in the CIP-007 redline do not match the changes in Project 2016-02. Tacoma Power recommends updating these tables to align with the recent CIP-007 draft in Project 2016-02.
- Table R1: Part 1.1 and Part 1.2 need to be updated. Part 1.3 is missing from Table R1.
- Table R2: Parts 2.1 through 2.4 need to be updated.
- Table R3: Parts 3.1 through 3.3 need to be updated.
- Table R4: Parts 4.1 through 4.4 need to be updated.
- Table R5: Parts 5.1 through 5.7 need to be updated.
- The Violation Severity Levels table should also be updated to align with the Project 2016-02 changes.
- Table R6, Parts 6.1 through 6.7 should include this statement at the end of the Applicable Systems list: “SCI supporting an Applicable System in this Part.”

Other Editorial Comments:

- “C. Regional Variances” should be “D. Regional Variances”
- The Section E, Interpretations, is missing. Recommend adding this section.
- “D. Associated Documents” should be “F. Associated Documents”.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	
Document Name	

Comment

The SRC notes that Parts 6.5 and 6.7 use different phrasing than the remaining parts of Requirement R6, and recommends that Parts 6.5 and 6.7 be revised to begin with "Implement one or more process(es)..." to better align with the language used in the rest of Requirement R6.

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 RSC

Answer	
Document Name	

Comment

It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1.

Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	
Document Name	

Comment

It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1.

Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access

monitoring", or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining "electronic access monitoring" as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	
Document Name	

Comment

Avista agrees with EEI's comment:

EEI suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	
Document Name	
Comment	

It is unclear why the SDT did not incorporate the proposed CIP-007 R6 Requirement into already existing Standards. Logging and log evaluations could have been added to CIP-007 R4, and malicious/anomalous activity capturing and evaluation could have been added to CIP-007 R3.

With regards to CIP-007-X R6.3, if an entity were to add a new system into its environment, how long would it have to be compliant with creating a new baseline? This is not clear in the proposed Requirement.

CIP-007-X R6.6 states, “Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.” What constitutes “sufficient detail and duration”, and how would that be audited?

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to “that has bypassed other electronic security controls”.

EEI suggested adding “in Part 6.2” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.

Technical Rationale Comments

BCSI Implications (see Classification Rationale, Page 3)

For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

Data Collection Methods, Pages 9 through 10

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

We support additional commentary as provided by EEI and NSRF.

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	
Document Name	

Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	

Avista agrees with EEI's comment:

Comments: EEI suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	
Document Name	

Comment

In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the of the SDT:

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network.
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	
Document Name	

Comment

The technical rational and guidance need more clarity to align auditors and implementors.

INSM system will have to meet the definition of EACMS as it performs electronic access monitoring function. It is unclear why there was an option not to classify it as EACMS but only BCSI. Clarity is required.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
Part 6.6 necessitates an explicit definition of data retention requirements. The current specification, which mandates retention with "sufficient detail and duration to support the investigation of anomalous activity," introduces a potential challenge. The determination of what constitutes sufficient detail and the appropriate duration is contingent upon the detection and subsequent investigation of anomalous activity. This approach poses a risk of non-compliance in scenarios where anomalous activity is identified after the data has been discarded. To mitigate this risk, it is advisable to allow for flexibility in retention periods, tailored to the specific nature of the data. For instance, considering the substantial volume of packet captures, it may not be pragmatic to retain them for extended periods. A more nuanced approach that accommodates variations in retention periods for different types of data would enhance practicality and adherence. We recommend consolidating the proposed Requirements into one or two cohesive Requirements. Additionally, GSOC believes that addressing this requirement within the framework of CIP-005 may be a viable and more streamlined alternative. This consolidation and alignment could contribute to a more coherent and manageable regulatory framework	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the SDT:	

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network?
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	
Document Name	

Comment

WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	
Document Name	

Comment

There are some concerns about CIP-007-X R6.3, how often does an entity analyze the traffic? Is it weekly, monthly, or would an instant alert be required. Without a little more direction an auditor and entity may disagree on the frequency.

Likes 0	
Dislikes 0	

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	

Document Name	
Comment	
The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. CEHE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	
Document Name	
Comment	
Scope of Requirement Parts: The SDT has a diagram of many EACMS and PACS communications with various forms of communication either in or out of scope represented by blue/red arrows. Southern Company suggests the diagram is not clearly represented in the requirement part scope language. For example, the diagram says the communications within a PACS out to its controllers is not in scope, however the requirement scope only states that PACS are in scope (those that rely upon an EACMS for access control). Once a PACS meets that condition, then the entirety of the PACS is in scope, which includes its distributed controllers as the requirement part itself explicitly says “between applicable Cyber Assets” within these systems (the PACS definition only excludes the badge readers, etc. at individual doors). That could be hundreds of widely distributed controllers across the enterprise in scope of this INSM requirement because the PACS is in scope and the main sentence of the requirement is written to “visibility between all applicable Cyber Asset” level, not the system level. There are huge implications of the Cyber Asset granularity rather than monitoring the communications to/from the PACS as a singular system. The SDT diagram is based on communications between systems, but the scoping of the requirement is visibility of all the applicable Cyber Assets within those systems and thus all communications to or from each individual programmable electronic device are in scope. While it states 100% is not required, it seems it is then left as an exercise to the entity to prove why they do not monitor 100% if they only monitor the PACS database server for example. This construct is quite prone to differences of opinion and perceived risk in audits. As another example, only EACMS that perform access control functions are in scope, but once in scope, then the visibility of all communications between all of its applicable Cyber Assets are in scope, thus all the arrows to any such EACMS are included. The scoping in the standard tells the entity what systems are in scope, but then its focus is monitoring the networks on which those systems reside which will include all comms to/from those systems. It is unclear in the scoping language how that allows for the red “out of scope” arrows. Southern Company suggests that the requirements be left at the BCS, EACMS, and PACS level, without mention of Cyber Asset within the requirement part language, which would more clearly allow entities the flexibility to monitor to the level of granularity within these systems that provides monitoring value commensurate with the expense and reliability impact of individual components. In the PACS example, the greatest security monitoring value may be for the database server containing the access rights database, but little value in monitoring hundreds of distributed controllers controlling individual doors in facilities across the entity’s footprint. We suggest this would help avoid the “monitor all, but 100% is not required” concept in the current language.	

Part 6.2: Southern Company suggests this requirement part is unnecessary (it is covered by 6.6), raises many questions, and adds evidence burden with no direct reliability benefit. It is a necessary step in the monitoring *process*, but not a security objective for a standard. We suggest stating the expected result of INSM rather than step by step procedural "how". Explicitly requiring a "collect the needed data" as a requirement requires not only an evidence burden, but brings with it all the questions of missing data, temporarily malfunctioning equipment, data retention to prove the logging is 100% complete, etc. We suggest deletion of this part.

Overall: Are all security objectives for the internal network inside the ESP also required of the systems outside the ESP in the "CIP Networked Environment?" For example, if the EACMS or PACS in scope are on the corporate network, does CIP-007 R6 require the detection of new devices or connections on the corporate network as well?

Vendor Support: This section of the Technical Rationale and SDT presentations explicitly denies any "per system capability" or allowance for vendor issues where they may not allow for modification of tightly engineered and integrated control systems that are maintained and/or warranted by the vendor. The statements that entities should upgrade due to monitoring requirements, where many control system upgrades at plant locations can begin in the $250,000 range and up, we suggest are overreach into large business/operational decisions that should be made by site management in view of all reliability risks that are being managed. With 6.1 currently stating 100% is not required, it seemed odd to have these "no exceptions based on vendor or system capability" type statements in the TR documentation that further cloud what is a compliant scope.

Examples: Southern Company suggests something that will greatly help the entities understand the INSM requirements is to lay out an example of a 1500MW Combined Cycle generation unit that has medium impact BCS, such as 3 separate multi-layered gas turbine control systems for 3 gas turbines, a different multi-layered turbine control system for a heat recovery steam turbine/generator, and a multi-layered DCS for Balance of Plant (BOP) operations – each of these a multi-layer Perdue model system all on one generating unit. Another example that would help is a large, 1500MW+ offshore wind farm with 200+ individual wind turbines. Thinking through examples such as these and what would be a compliant INSM implementation will help the SDT with scoping requirement parts such as 6.1 as well as helping the industry and CMEP personnel understand what a compliant INSM implementation is, not just in data centers and substation control houses, but in the large industrial plant scenarios within the BES.

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment

The term "CIP-networked environment" is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. SIGE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	

We appreciate the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Regarding CIP-008, We urge the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point.

Lastly, we thank the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	
Document Name	
Comment	
We are concerned with the statements the SDT has included in the Technical Rationale regarding Vendor Support where they state on page 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” The SDT stating that “every control system should have the capability to provide an appropriate level of visibility” and suggesting that entities will need to update them with modern equipment is unreasonable and may present new risks through new attack vector points into previously isolated systems. This is also in direct contradiction to Requirement R6.1 that allows the entity to assess what level of INSM provides “security value”. Without providing a minimum threshold for monitoring or further guidance on what provides “security value”, there is a lot of room for interpretation into what is required for an entity to meeting compliance with Requirement R6. For those entities that are operating in regulated environments, there is also the possibility of negatively impacting rate payers through costs associated with stranded assets. Including communication between EACMS and PACS systems within the scope of the requirement can create additional obstacles where the systems are managed separately on different networks. There is no guidance provided on how to treat INSM devices that could act as a possible bridge between networks, which would impact compliance with CIP-005.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No other comments	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-03 Internal Network Security Monitoring | Draft 1
Comment Period Start Date:	12/14/2023
Comment Period End Date:	1/17/2024
Associated Ballot(s):	2023-03 Internal Network Security Monitoring (INSM) CIP-007-X IN 1 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-007-X Non-Binding Poll IN 1 NB 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 75 sets of responses, including comments from approximately 198 different people from approximately 116 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, Soo Jin Kim (via email) or at (404) 446-9742.

Questions

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry. Industry largely agreed that the language in FERC Order 887 was clear on the inclusion of high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC.

The DT did receive the comment that "excluding low impact BCS presents a moderate level of risk and vulnerability." The DT appreciates this comment, however, the Project 2023-03 SAR scope is for the DT to "…create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order," (FERC Order 887). "The scope of the project will include:

- All high impact BES Cyber Systems, and
- All medium impact BES Cyber Systems with ERC.

The scope of the project should not extend to:

- Medium Impact BES Cyber Systems without ERC, or
- Low impact BES cyber systems."

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

Summary Responses:

The DT vetted comments received from industry. Industry comments centered largely around concerns regarding the Draft 1 CIP-007-X applicability section related to EACMS and PACs outside the ESP. The DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The DT determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolve the concerns expressed by industry. Note that communications between BCA, PCA, EACMS and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

3. Order No. 887 also references "CIP-Network Environment" that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry. Similar to Question 2, industry comments addressed the applicability section of CIP-007-X. The DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP and the scope of the standard should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolve the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry and appreciates the valuable feedback received regarding this question. Numerous comments expressed support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach.

Industry concerns were raised regarding the usage of the phrase, "100 percent coverage is not required," and certain other subjective terms. To address these concerns, the DT made modifications to CIP-015, Requirement R1, Part 1.1 by removing the phrase, "100 percent coverage is not required," and including the phrase, “Based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, the DT added guidance to the measure for the documentation of the rationale for selecting or excluding monitoring locations. Moreover, the DT revised the Technical Rationale based on industry feedback pertaining to this aspect of the requirement.

5. The Project 2023-03 SDT held extensive conversations about the term “baseline” and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT’s use of the term “network communications ‘baseline’” is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry and removed the term “baseline” from the requirement language and moved it into the Measures section for the Draft 1 CIP-015-1. Additionally, the language of the requirement has been changed to focus on detection of anomalous network activity. The DT believes these changes alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies. Additionally, the DT sought to not inhibit use of new

technologies and left the retention period and scope at a high level to allow the Responsible Entity to determine what is reasonable. The language, "Sufficient detail and duration to support analysis," in the CIP-015 draft is intended to support that not all data is required to be retained.

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term "anomalous." The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of "anomalous" was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term "anomalous" was the appropriate term to use to describe that methodology. Do you agree that that the term "anomalous" effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry and had numerous discussions on the usage of, and alternatives to, the word "anomalous" and the phrase, "Indicative of an attack in progress." In the drafted CIP-015 requirements, the DT believes the several changes made address industry's concerns about scope. First, the scope of the requirements was reduced to applicable systems within the ESP. Second, the DT added language for identifying collection locations and methods, "That provide value, based on the network security risk(s)." Additionally, the subsequent requirement is to, "Detect anomalous activity using the data collected at locations identified." The DT believes these changes provide entities with flexibility and helps create limits on what data needs to be collected and evaluated.

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT vetted comments received from industry and revised CIP-015, Requirement R1, Part R1.3 (formerly CIP-007, Requirement R6, Part R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The

word anomalous was removed from the section; however, the intent of Requirement R1 is, "…To improve the probability of detecting anomalous or unauthorized network activity." Accordingly, the addition of the word "potentially" is not warranted to qualify "anomalous". Additionally, Page 4 of the Technical Rationale states, "Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." In turn, this allows entities to determine which anomalous activity is determined to be malicious or innocuous. The DT believes the changes satisfy the concern of industry's comments.

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

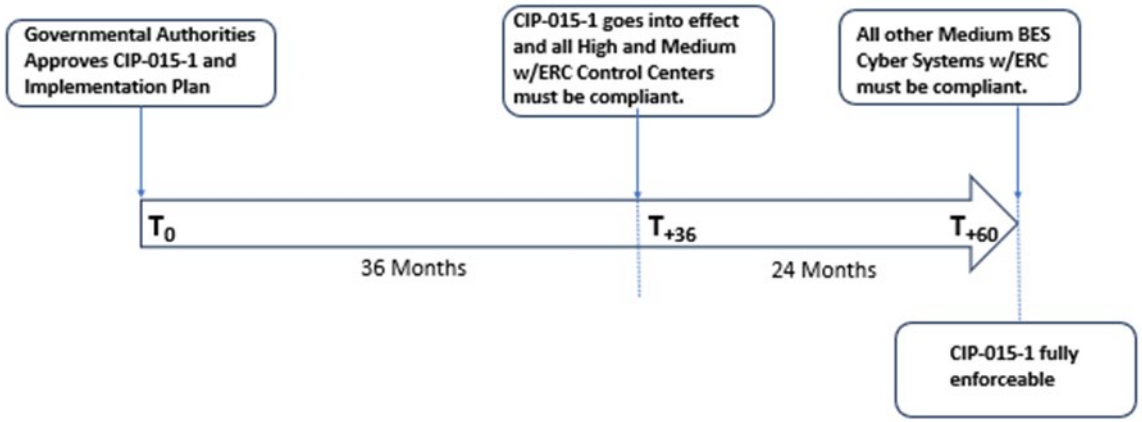
Summary Responses:

The DT vetted comments received from industry, which mostly centered around concern for entities to not have enough flexibility in using various INSM methodologies and technologies. The DT believes the current revision in CIP-015 addresses these comments. While the implementation does require network collection and analysis, the DT updated the Technical Rationale to reflect additional methods of analysis and to ensure that various tools can be used to comply with the newly drafted CIP-015 standard. Additionally, CIP-015, Requirement R1, Part R1.1 allows entities the ability to collect data in a way that can monitor systems that may not have a built-in capability. Note that network data must be collected, but the language allows entities and vendors wide latitude to collect necessary data.

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Summary Responses:

The DT appreciates all the comments received from industry and created a graph to help clarify the implementation timeframes.



10. **Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.**

Summary Responses:

The DT vetted comments received from industry and agreed the standard does not support inclusion of EACMS and PACS outside of the ESP, which reduces the economic impact to industry. Additionally, the DT revised the CIP-015, Requirement R1, Part R1.1 (formerly CIP-007, Requirement R6, Part R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.

11. **Please provide any additional comments for the SDT to consider, if desired.**

The DT is appreciative of numerous comments received by industry. The DT revised requirement language to allow entities to determine their own retention processes. Additionally, the DT addressed the standard's scope to limit applicability to High and Medium Impact BES Cyber

Systems and their EACMS and PACs networks within the ESP. Note that communications between BCA, PCA, EACMS and PACS within an ESP are still in scope and should be considered during any INSM implementation. CIP-012 communications are between ESPs and are not in scope.

This standard is very clear that an INSM system is not automatically designated as EACMS. As stated in the Technical Rationale, INSM systems are a poor choice for monitoring electronic access to an EAP because an INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems which very accurately detect failed or successful logons. If an entity uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is a likely designation for that entity. An entity that can monitor electronic access using other tools would not need to designate their INSM as EACMS. The CIP-015 standard leaves that designation up to each entity.

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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					George Brown	Pattern Operators LP	5	MRO

					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities- Kansas (BPU)	1,3,5,6	MRO
Anne Kronshage	Anne Kronshage			Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC

					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Southern Company - Southern Company Services, Inc.	Colby Galloway	1,3,5,6	MRO,RF,SERC,Texas RE,WECC	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
					Leslie Burke	Southern Company - Southern Company Generation	5	SERC
Jay Sethi	Jay Sethi		MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
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
					Mark Garza	FirstEnergy- FirstEnergy	1,3,4,5,6	RF

					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
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
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC

Black Hills Corporation	Rachel Schuldt	6		Proj 2023-03 INSM	Rachel Schuldt	Black Hills Corporation	6	WECC
					Micah Runner	Black Hills Corporation	1	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Josh Combs	Black Hills Corporation	3	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC

John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC

					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	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
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
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC

					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
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
					Gary Dollins	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC

					Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
					Jarrod Murdaugh	Sho-Me Power Electric Cooperative	3	SERC
Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene Free	Santee Cooper	1,3,5,6	SERC
					Christie Pope	Santee Cooper	1,3,5,6	SERC
					Chris Mcneil	Santee Cooper	1,3,5,6	SERC
					Troy Lee	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Jordan Steele	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC

					Shedrick Snider	Santee Cooper	1,3,5,6	SERC
					Kevin Gainey	Santee Cooper	1,3,5,6	SERC
					Lachelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
1. The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications. 2. The standard should be focused on BES Cyber Systems and PCAs (e.g., those systems inside the ESP). Inclusion of non-BES Cyber Assets, coupled with the ambiguity of non-glossary defined criterion is overly broad and diminishes the focus on protecting the most important systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDT responses to comments received for Question #3 regarding how the SDT has addressed the scoping language.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	

With the increased concern of critical infrastructure infiltration by foreign adversaries, excluding low impact BCS presents a moderate level of risk and vulnerability.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 SAR scope is for the DT to "…create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order," (FERC Order 887). "The scope of the project will include:

- All high impact BES Cyber Systems, and
- All medium impact BES Cyber Systems with ERC.

The scope of the project should not extend to:

- Medium Impact BES Cyber Systems without ERC, or
- Low impact BES cyber systems."

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see the responses to NPCC's comments for Question #1.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see the DT responses to comments received for Question #3 regarding how the DT has addressed the scoping language.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) believes the proposed language does not explicitly exclude low impact BCS and medium impact BCS without ERC, it does not mention low impact. It explicitly includes applicable systems, but it does not explicitly exclude anything.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT appreciates this comment, however, the Project 2023-03 SAR scope is for the DT to "…create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order," (FERC Order 887). "The scope of the project will include:

- All high impact BES Cyber Systems, and
- All medium impact BES Cyber Systems with ERC.

The scope of the project should not extend to:

- Medium Impact BES Cyber Systems without ERC, or
- Low impact BES cyber systems."

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the response to MRO's comments for Question #1.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 current language in Draft 1**.**	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees it is clear that low impact BCS and medium impact BCS without ERC are not included in the proposed requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: "EEI agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC. "	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments	

Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you. Please see response to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	

Answer	Yes
Document Name	
Comment	
Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	Yes
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	
See comments submitted by the Edison Electric Institute	

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	

Comment

We appreciate the effort of the SDT in trying to interpret FERC Order No. 887 and revise the CIP standards to address it appropriately. We agree that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the "CIP-networked environment" diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP. PACS communication systems may be configured in such a way that it is completely separate from the OT environment. By including communication between EACMS and PACS, the standard could unintentionally be increasing the scope of many CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Please note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees that Order 887 explicitly included high impact BCS and medium impact BCS with ERC. However, the question concerns the 'cyber assets included in the standard' which is a larger scope. Given the unclear scoping of 6.1 as currently written, requirement part 6.1 itself, the diagrams showing some 'out of scope' PACS components, and statements in the TR that state that not all Cyber Assets involved will be of sufficient monitoring value to include, Southern Company concludes that not every Cyber Asset in the 'CIP Networked Environment' should be included in mandatory scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	

Answer	No
Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

It is unclear why EACMS that perform only monitoring function are excluded from the requirements. An EACMS that only monitors, such as SIEM, could be compromised should there be any deletion or modification of logs concealing the malicious activities or traffic. Thus, it should also be included in order to improve the reliability.	
Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

The Project 2023-03 SAR scope is for the DT to "…create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order," (FERC Order 887). "The scope of the project will include:

- All high impact BES Cyber Systems, and
- All medium impact BES Cyber Systems with ERC.

The scope of the project should not extend to:

- Medium Impact BES Cyber Systems without ERC, or
- Low impact BES cyber systems."

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No

Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
While PNMR agrees with the cyber assets included within the standard, it does not necessarily believe that this requirement as a whole increases reliability but more so, security.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
The question is somewhat unclear. Interpreted as if there is a subset of “scoping” besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The “scoping” mechanism is unclear when reviewing the proposed CIP-007 R6.1. It is also unclear what “will further reliability within the CIP-networked environment”. How would this be measured? Is this purely subjective? A Responsible Entity could disagree. EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the	

scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

The Project 2023-03 SAR scope is for the DT to "…create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order," (FERC Order 887). "The scope of the project will include:

- All high impact BES Cyber Systems, and
- All medium impact BES Cyber Systems with ERC.

The scope of the project should not extend to:

- Medium Impact BES Cyber Systems without ERC, or
- Low impact BES cyber systems."

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

The question is somewhat unclear. Interpreted as if there is a subset of "scoping" besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The "scoping" mechanism is unclear when reviewing the proposed CIP-007 R6.1.

It is also unclear what "will further reliability within the CIP-networked environment". How would this be measured? Is this purely subjective? A Responsible Entity could disagree.

EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy notes that the defined term BCS is inclusive of devices classified as BCA and not other associated classified cyber assets, and therefore agrees with the BCS that were selected for inclusion. However, Duke Energy does not agree that the additional cyber assets included in the proposed standard's applicability further reliability within the CIP-networked environment. We do not support the	

interpretation that the CIP-networked environment is inclusive of EACMS and PACS-classified cyber assets that do not reside within an ESP. Since V5 took effect, the only constructs for trust zones defined within the CIP standards are the ESP applicable for High/Medium BCS and the Low Electronic Access Controls required by CIP-003 Attachment 1 Section 3. There is no trust zone that the standards contemplate for EACMS and PACS devices that reside outside the above identified zones. Therefore, the intention to monitor east-west traffic within a trust zone in FERC Order 887 most clearly fits with the expectation that INSM is applied within applicable ESPs to increase network visibility beyond the existing perimeter-based controls required by CIP-005. Moving beyond the BCS and outside the ESP takes the focus off the most critical environments for monitoring. INSM systems are likely to generate extreme volumes of data as entities mature their implementations. Large data volumes will require significant investment of time and resources to generate meaningful baselines of network traffic, especially for large entities with diverse software solutions across their various BCS and EACMS. An unclear and overly large scope for the initial INSM implementation threatens to create alarm/alert fatigue that will hamper the ability of entities to detect and respond to threats to their most critical systems residing within their ESPs.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No

Document Name	
Comment	
FERC Order 887 did not include EACMS and PACS. There is no requirement that EACMS or PACS be protected by a firewall, so to include them as part of "inside the CIP-networked environment" is a huge stretch for the Standards Drafting Team to make and scope creep of Order 887. Including EACMS and PACS in the requirement for INSM, where monitoring is only required between them, does not further the reliability and security inside the CIP networked environment. There is likely to be a lot of "noise" that must be tuned out when trying to monitor only traffic between certain EACMS and PACS devices since they can be inside more open networked environments. The security value of monitoring only the "INSM" (east-west) traffic assumes that you must first be compromised by non-INSM (north-south) traffic before you would potentially see anomalous INSM communication; this makes very little security sense.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	

Comment
EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Please see the response to NPCC's comments for question #2.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The "CIP-networked environment" diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS, and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for question #2.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for question #2.	
Daniel Gacek - Exelon - 1	
Answer	Yes

Document Name	
Comment	
Exelon is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for question #2.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for question #2.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the question refers to CIP-networked environment, which has created confusion about the SDT's goal for responses. To refer to a CIP-networked environment high impact BCS and medium impact Cyber Assets with ERC does not align with current CIP-005 language in R1.1 which requires medium and high	

impact BCS and their associated Protected Cyber Assets “connected to a network via a routable protocol shall reside within a defined ESP.” Inclusion of EACMS and PACs in the standard draft language goes beyond Order No. 887.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Please see the response to SRC’s comments for question #2.	

Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI is of the opinion that the proposed changes will improve the security of the CIP-networked environment. “	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI’s comments for question #2.	
Kimberly Turco - Constellation - 6	

Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 cyber assets included within the standard will further reliability within the “CIP-network environment”**.**	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Please see the response to MRO's comments for question #2.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes R6.2 could conceivably lower security posture if the transport and/or repository of such logging information is compromised.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT team recognizes there is some risk if the INSM infrastructure is compromised. The security benefits to having an INSM program outweigh those risks. The DT team has addressed concerns over unauthorized deletion or modification in the CIP-015.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
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	

Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes that whether any other ballot pool member agrees with the directives in Order 887 is moot. Questions about what types of BCS should or should not be addressed by revisions to one or more CIP Standards should have been raised after FERC issued its Notice of Proposed Rulemaking about INSM on January 27, 2022.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.

3. Order No. 887 also references "CIP-Network Environment" that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	

Comment

The scoping of PCA is clear. However, the language "that perform access control functions" is not clear. The language would be improved by specifying what type of "access control functions" are applicable (e.g., for authentication). Consider the following revisions for the High and Medium Impact scoping language in the Applicable Systems section:

1. EACMS that perform authentication functions;

2. PACS that rely upon EACMS that perform authentication functions; …

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications. As the standard in current state does not direct that PACS be protected by an EACMS, entities are dis-incentivized to protect PACS due to the additional regulatory exposure created by the draft language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	

Answer	No
Document Name	
Comment	

While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	

OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Please see the response to the NPCC Regional Standards Committee's comments for Question #3.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn't clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don't feel the term CIP-Network Environment should be used here when it can't be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn't where entities should be getting that information. Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the	

scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

BPA supports Chelan PUD's remarks proposing modification of the draft scoping language in the Table R6 – INSM - Applicable Systems section to reduce confusion about which EACMS and PACS are in scope:

1. EACMS that perform authentication functions;

2. PACS that rely upon EACMS that perform authentication functions; …"

For clarity, BPA also recommends the drafting team reinstate the definitions pertaining to "Applicable Systems" on page 6 to include definitions for any new terms used in the next draft, especially the phrase "PACS that rely upon…"

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP

successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The Standard Drafting Team has done a very good job at identifying additional components in the “CIP-Network Environment” that need to be monitored without increasing the scope further than necessary. The technical rationale describes the scope, including a diagram. The language used in the applicability section EACMS “that performs access control functions” does not match the diagram and intent of the Standard Drafting Team. This phrase would include all access control EACMS, including the following that were marked as out of scope on the diagram: An EACMS that contains an EAP, for example a firewall An EACMS that acts as an Intermediate System, for example a jump host To clarify the EACMS in scope it is suggested to use the wording “EACMS that perform authentication for more than one CIP Cyber Asset”. This better matches the diagram presented, where traffic going to a firewall (an access control EACMS) is out of scope, however traffic to a two factor authentication server or active directory server would be in scope. Manitoba Hydro suggests removing PACS from the applicability section, as there are no other network security requirements that apply to PACS. Traffic from EACMS that support PACS would already be included if the EACMS was in scope.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Please see the response to the MRO group's comments to Question #3.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E does not agree the language clearly indicates what is in-scope and out of scope. The FERC Order was for "internal" communications, but the current language does not clearly indicate this and could be interpreted by auditors to include traffic outside of the ESP, such as those to PACS and EACMS outside of the ESP. PG&E recommends to clearly indicate that communications outside of the ESP to devices such as PACS and EACMS are not in scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE is concerned with scoping EACMS to only those that perform access control in Requirement R6. Certain monitoring systems, such as a SIEM, may be an attack priority and should be included in internal network monitoring. SIEMs contain logs for all CIP networked devices configured to send applicable security logs to them. An attack against the SIEM could subsequently result in an attacker removing logs of	

their activity in order to prolong time to discovery and hinder recovery efforts. Texas RE recommends removing the language "that perform access control functions" from the Applicable Systems column. Texas RE noticed the SDT identified “PACS that rely upon EACMS that perform access control functions” as an Applicable System in Requirement R6. Texas RE requests clarity on what this is intended to be mean. Texas RE noticed the technical rationale document states “CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device is out of scope.” (Page 6). The technical rationale should not create or modify requirement language. If these types of communications are intended to be out of scope, this should be represented in enforceable requirement language, either by explicitly defining what communications are in scope or by explicitly defining what communications are out of scope.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	
Comment	
The order does not specifically reference EACMS and PACS, therefore it is not part of the CIP-network environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	
Comment	
Oncor stands in agreement on the comments made by EEI that states: "EEI remains concerned that the applicability section for Requirement R6 is not sufficiently clear and needs additional work in order to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested some edits to the applicability	

section in our response to question 4, further work may still be needed beyond replacing “access control” with “authentication control”. Nevertheless, we do feel authentication control is superior to access control, as proposed."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. Please see responses to EEI’s comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with MRO provided comments: "While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS).	

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolve the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
FERC Order 887 references a CIP-Network Environment in the context of assets within an Electronic Security Perimeter. The Order does not mention PCA, EACMS, or PACS. The standard language including those devices is a significant expansion of the scope of the FERC Order. While PCA are, by definition, within the Electronic Security Perimeter, EACMS and PACS are not necessarily located within the ESP and should not be included in the standard.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

As documented in FERC Order 887, "INSM is a subset of network security monitoring that is applied within a "trust zone," such as an electronic security perimeter. For the purpose of this rulemaking, the trust zone applicable to INSM is the CIP-networked environment," the trusted zone protected by a firewall. Including EACMS and PACS, which are not required to be protected by an ESP, Electronic Access Point (EAP), or required to be in a "trust zone" does not align with intent of the SAR or the FERC Order, which is to perform network monitoring of traffic between devices ***within*** a trusted zone.

The intent of the SAR was to close the gap that currently exists in CIP-005, which is the inability to detect lateral movement of a compromised system. The way the requirements are currently scoped, EACMS and PACS are included when they are not even required to be in a trusted zone, and only traffic between them proposed for monitoring. Therefore, this becomes a detective control to determine if a device has already been compromised.

EACMS and PACS should be removed from the project scope and the INSM requirements should be moved to CIP-005. Including EACMS and PACS in the scope, significantly increases the cost and complexity of the INSM requirement as many PACS are spread throughout different

geographical locations and networks, significantly increasing the cost and complexity of implementing the requirements, with little security benefit to gain since any attack would likely come from a Cyber Asset that is not classified as an EACMS or PACS. SMUD recommends removing EACMS and PACS from the project scope and moving the INSM requirements to CIP-005 as a network and BCS level control rather than leaving it in CIP-007 where Cyber Asset level controls are typically required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. The DT created this new CIP-015-1 standard specifically for INSM requirements and moved it out of CIP-007-X. A new standard will allow for future drafting teams that consider INSM in other BES Cyber Systems a basis to work from going forward.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy's understanding of the CIP-Networked Environment and its use in the order was that it meant to capture High BCS and Medium BCS without ERC, while using language that could align in the future with the requirement for Lows for which there is no ESP. With that disclaimer, we believe that the applicability clauses " EACMS that perform access control functions" and "PACS that rely upon EACMS that perform access control functions" is meant to convey a subset of EACMS and PACs, and it is unclear exactly which subset of these assets is	

intended to be included. This applicability will necessitate entities performing subclassifications of their EACMS and PACS to determine potential scope. We recommend the Applicable Systems be scoped to High Impact BES Cyber Systems and their associated PCA and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA. If the SDT is unable to align to this approach that leverages the existing CIP-required trust zones, we would request that the SDT invest the necessary time to define terms to clearly articulate which subsets of EACMS and PACS are relevant for this standard.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	

Comment
Without discouraging implementation of ISNM, the administrative burden of classifying the NERC-defined term of EACMS more granularly diminishes the value the SDT intended. The reliability gained by requiring INSM on this subset of systems does not outweigh the increased cost or additional documentation needed to prove compliance.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolve the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Please see the response to the MRO NSRF comments for Question #3.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Please see the response to the EEI comments for Question #3.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI comments: " The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project. "	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST believes Order 887 is clearly intended to apply exclusively to high or medium impact BCS inside ESPs, its use of the phrase, "CIP-networked environments" notwithstanding. There is no mention in the Order of "CIP" devices that may be outside ESPs, such as EACMS and PACS, and we believe this was in fact intentional. We note, further, there are numerous statements in the Order that reinforce this opinion, including:

"INSM is a subset of network security monitoring that is applied within a 'trust zone,' such as an electronic security perimeter." (Paragraph 2)

"We find that, while the CIP Reliability Standards require monitoring of the electronic security perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack." (Paragraph 3)

"Finally, INSM provides insight into east- west network traffic happening inside the network perimeter, which enables a more comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone." (Paragraph 13)

"The NOPR explained that including INSM requirements in the CIP Reliability Standards would ensure that responsible entities maintain visibility over communications between networked devices within a trust zone rather than simply monitoring communications at the network perimeter access point(s) (***i.e., at the boundary of an electronic security perimeter as required by the current CIP requirements***)." (emphasis added) (Paragraph 14)

"While the CIP Reliability Standards require monitoring of inbound and outbound internet communications at the electronic security perimeter, the currently effective CIP Reliability Standards do not require INSM *within* trusted CIP-networked environments for BES Cyber Systems." (Paragraph 20)

In addition, the Q2 2023 issue of the highly respected and widely consulted ReliabilityFirst newsletter, "The Lighthouse," is titled, "Preparing for Internal Network Security Monitoring (INSM)." It opens with the following statements: "Internal Network Security Monitoring, or INSM, is the practice of understanding what is going on inside your networks. For the purposes of the CIP Standards, that means understanding what network traffic is occurring ***within*** your Electronic Security Perimeters (ESPs)." (emphasis added). With all due respect to the SDT's "risk-based approach" (not described in the Technical Rationale document) to deciding certain types of CIP devices outside of ESPs should** be in scope, NST believes the drafting team has far exceeded the authorization granted by the Standards Committee's approval, on August 23, 2023, of the INSM Standard Authorization Request.

** NST notes that on Page 5 of the Technical Rationale document, the SDT states, "The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) ***shall*** be inclusive of the following (adjusted for clarity for the purposes of showing SDT development of revisions to CIP-007-X):" (emphasis added). We assume the use of the word, "shall" was unintentional.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Jennifer Neville - Western Area Power Administration - 6

Answer	No
Document Name	

Comment

Need to clarify which EACMS provide “access control” only. Consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”. Also please clarify that only authenticating EACMS need to be included or update the language under Applicable Systems to explain.	
Likes 0	
Dislikes 0	

Response

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

Entergy has concerns regarding the Applicable Systems of the proposed standard and the use of new terms and/or scope increase, in particular with “PACS that rely upon EACMS that perform access control functions”. It is not clear on what “rely” means in this context. Additionally, this would expand scope beyond network security requirements for PACS, or incentivize entities to reduce security for compliance margin. For example, under the existing CIP-005 standard PACS are not required to reside in an ESP or have their External Routable Connectivity flow through an Electronic Access Point on an EACMS. Under this standard an entity could utilize a non-CIP interface on a EACMS with a segmented network to provide perimeter protections/access control as a best security practice, but this would be outside CIP-005 scope. With the proposed standard as drafted because that EACMS is providing security controls to the PACS, even though not

required by CIP-005, the PACS would be brought into scope of this standard. This could incentivize entities to move PACS away from EACMS systems providing access control to less secure pathways totally outside CIP scope to avoid an increase in compliance requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS. Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review. Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be:	

Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that the devices (e.g. PCA, EACMS, and PACS) are included or excluded for INSM data collection consistent with Order No. 887. Question 3 indicates "The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets" which appears to be missing a part of the statement. How did the SDT team risk-based approach exclude EACMs and PACs that are only performing monitoring functions? As described in the technical guidance, "Threat actors commonly take steps to hide their actions, and very often need to work for an extended period within targeted environments to develop disruption capabilities." In either case, the NAGF would refer the SDT back to Order 887 in that the network traffic in scope for INSM is communications within an ESP between other Cyber Assets within that "trust zone" also referred to as	

east west traffic. The inclusion of EACMS and PACS goes beyond the scope of INSM and the current Draft 1 creates confusion as to the intent of the requirements commingling “Network Security Monitoring” principles which include devices outside of the ESP or “trust zones”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	
Tacoma Power does not agree with the addition of EACMS and PACS to this Standards Project. While Order 887 specifically calls out the “CIP-Networked Environment”, there is no mention of EACMS or PACS in the Order. In reviewing previous FERC Orders that have applied to EACMS and PACS, these system types are specifically identified within the Order, see FERC Order No. 850 as an example.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

Is this question asking to "scope" the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?)

Please clarify if the evaluation approach is CIP-007 R6.1 "…Collection methods should provide security value to address the perceived risks."

Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing.

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn't clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don't feel the term CIP-Network Environment should be used here when it can't be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn't where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. Please see DT responses to comments received for Question #4 regarding how the DT has addressed the "100% coverage is not required" language.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	

Response	
Please see the response to EEI's comments for Question #3.	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS. Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review. Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be: Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Is this question asking to “scope” the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?) Please clarify if the evaluation approach is CIP-007 R6.1 “…Collection methods should provide security value to address the perceived risks.” Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing. The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don’t feel the term CIP-Network Environment should be used here when it can’t be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn’t where entities should be getting that information. Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. Please see DT responses to comments received for Question #4 regarding how the DT has addressed the "100% coverage is not required" language.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the "CIP-Network Environment" then it should be out of scope as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
The definition for EACMS currently reads, “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.” PNMR understands the STD’s intent to focus on EACMS designed for access control, but specifically designating types of EACMS (and PACS) for the Applicable Systems seems to indirectly change definitions. This change also deviates from all existing “Applicable Systems” in current Standards. Additionally, to more closely align with language related to other “Applicable Systems” in other requirements, PNMR believes the “Applicable Systems” should read, “EACMS with access control functions.” Finally, PNMR is unclear on the exact meaning behind, “PACS that rely upon EACMS that perform access control functions.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No

Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Please see the response to the MRO NSRF's comments for Question #3.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for Question #3.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Please see the response to the MRO NSRF's comments for Question #3.	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for Question #3.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the "CIP-Network Environment" then it should be out of scope as well.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for Question #3.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	

Comment	
Please see LCRA's response to question 2 above. The term "CIP-networked environment" is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
The EACMS that perform only monitoring function should also been included. Although described in technical rationale, it is better to properly add "CIP-Network Environment" in NERC's glossary of terms.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The FERC order specifically addressed High and Medium-Impact assets. Extending the proposed standard to associated EACMS and PACS exceeds the scope of the FERC order and they should be removed. GSOC believes that the order as written could include communication between High or Medium assets and their corresponding PACS/EACMS. Nevertheless, there is a lack of clarity regarding the inclusion of ALL EACMS and PACS communications within the Applicable Systems. If the intent is to capture such communications, this can be feasibly achieved through tools already monitoring the High and Medium assets from within their ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Please see LCRA's response to question 2 above. The term "CIP-network environment" is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	

Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Please see the response to the MRO NSRF's comments for Question #3.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Consider defining "CIP Networked Environment" in the glossary of terms or the standard itself. Additionally, "CIP Networked Environment "could be further defined to make it clearer on what is included and excluded.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887. CEHE believes that the use of "EACMS that perform access controls" and "EACMS" from the "Interpretation of the CIP-Network Environment" diagram presented in the DT webinar is unclear. "EACMS" seems to refer to authentication mechanisms, but EACMS in some environments, if not most, refer to firewalls that do not perform authentication, but do perform access control. CEHE suggests using the phrase "EACMS that perform authentication functions" as it relates to the "CIP-Network Environment."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the comments by EEI. Additionally, Southern Company would like to state a concern for the record that the scope of the current draft does not clearly align with what is stated in the Order and the SAR. The only reference to EACMS and PACS in the Order is in section 21 and is in relation to the existing requirement CIP-007 R4.1.3. While it is clear in the Order that the scope of CIP-networked environment extends beyond the Electronic Security Perimeter, it would be helpful to industry in the future if all applicable Cyber Assets intended to be included were clearly stated in the Order and the SAR.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment
SIGE believes that “PACS that rely upon EACMS that perform access control functions” is not entirely clear. It is not clear what “rely upon EACMS that perform access control functions” means. It could be interpreted to mean the PACS relies on the EACMS to validate that an individual is allowed to have physical access to a NERC CIP area, or it could be interpreted to mean the PACS relies on the EACMS to validate a username and password in order to log into the PACS server/system. SIGE would like to see further clarification included.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the Technical Rationale, it isn't clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. We don't recommend using the term CIP-Network Environment when it can't be found in the glossary of terms. The diagram in the Technical Rationale is required for clarity on what the applicable systems are, but is still ambiguous enough that it leaves too much interpretation between systems that an entity identifies as applicable versus what an auditor would identify as applicable systems. Stating that 100% coverage is not required without providing a minimum threshold or other guidance on an acceptable level of coverage leads to potential confusion. Different entities define and evaluate acceptable levels of risk differently. If the RE determines that 50%	

coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Please see the response to EEI's comments for Question #3.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Prior CIP SARs have scoped a projects applicable system(s) by what is stated in the Project Scope section of a SAR. To rely on the undefined term “CIP-Network Environment” to further scope this project creates confusion for industry. The project scope of the SAR only listed – The Standard Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order. The scope of the project will include: • All high impact BES Cyber Systems, and • All medium impact BES Cyber Systems with ERC The scope of the project should not extend to: • medium Impact BES Cyber Systems without ERC or • low impact BES cyber systems	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	

MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC). In addition, MISO asks the SDT to consider adding the term "CIP-networked environment" to the NERC Glossary. As this term is used in FERC Order 887, defining it could be useful in identifying which EACMS (e.g. those used for authentication only and traversing the EAP) are applicable.

Likes 0	
Dislikes 0	

Response
Thank you for your support.

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	

Comment

To avoid numerous interpretations of if '100 percent coverage is not required' then what is required. Consider the following -

'Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets, as determined by the Responsible Entity, to monitor and detect anomalous activity. Collection methods should ensure visibility to identify known or suspected malicious communications.'

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the

documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
We agree that it is clear the way Requirement R6.1 is written that not every CIP network interface is required to be monitored with INSM. However, without providing a guidance document on what provides "security value" and is considered "critical" there is enough ambiguity that there can be disagreements between what an entity has identified within its own processes and procedures and what an auditor considers to be "critical" and provides "security value", leading to the auditor issuing PNCs. How can an auditor or entity determine they did enough? If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	

Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments filed by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC’s comments.	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	
Comment	

While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment
Southern Company agrees with the comments by EEI. In addition, Southern Company offers the following comments: Requirement R6.1 currently has an abundance of phrases that entities must prove with evidence. For example, it can be read that the entity must describe how *each* collection location or method can monitor and detect anomalous activity and specifically all connections, devices, and network communications. Southern Company suggests 6.1 be rewritten so that it does not force entities to "prove the negative" of the gap between what they did monitor and the 100% of all applicable Cyber Assets. The following wording is recommended to align with this concept: "One or more process(es) to identify network data collection locations the Responsible Entity determines provide sufficient security value in determining anomalous activity." With this wording concept, the evidence burden shifts to providing a reasonable monitoring location identification process and then evidence it was followed.

Likes 0	
Dislikes 0	

Response
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	
Comment	

While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.

Likes 0	
Dislikes 0	
Response	

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer	No
Document Name	
Comment	

CIP-007-X, Requirement R6, Part 6.1 indicates 100% is not required. This statement leaves a lot open for interpretation by an auditor. If an entity is collecting 50% of the data is it compliant or will an auditor determine this is not enough. Without a firm number communicated to auditors and entities it would be difficult to ensure Part 6.1 is interpreted the same way.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	

Thank you. Please see response to MRO's NSRF comments.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity's interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the language is still too vague to sufficiently inform LCRA's determination of the level of coverage necessary for compliance with the requirement.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Part 6.1 includes "network communications." However, the term introduces ambiguity as it is unclear which specific network communications require identification, such as protocols, ports, applications, or other elements.

The mandate for 100% coverage is not explicitly stated, creating uncertainty about the extent of coverage required. There is a lack of clarity in defining the parameters or criteria determining the necessary coverage.

The statement, "Collection methods should provide security value to address the perceived risks," prompts questions about the nature of the perceived risks. It raises considerations about whether it necessitates the formal execution of a risk assessment specifically targeting internal networks. Additionally, there is uncertainty about the expectation to document identified risks and articulate how an entity's data location and methods effectively mitigate these risks, extending beyond the implementation of INSM (Industrial Network Security Monitoring).

The measures proposed in the Standard imply that the sole requirement is the provision of architecture documents or similar documentation. If this interpretation is accurate, the language within the updated Requirement could be simplified to explicitly state, "Identify network data collection locations and methods designed to offer visibility of network communications (excluding serial) among relevant Cyber Assets." This modification would enhance precision and eliminate potential misinterpretations.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	
Comment	
It is not clear to the intent. “what is more critical to monitor” and “security value to address the perceived risks” is vague; additional details/specifics should be provided.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity’s interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the	

language is still too vague to sufficiently inform LCRA's determination of the level of coverage necessary for compliance with the requirement.	
Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith

Answer	No
Document Name	

Comment

AZPS does not believe the current language is clear in regard to performing an assessment of applicable CIP network communication and determination of what is most critical to monitor. AZPS recommends "Perform an assessment to identify locations and methods to collect network communication data (excluding serial) between applicable Cyber Assets, including connections, devices, and routable protocol network communications, to monitor and detect deviations from a normal network communications baseline. Identified locations and methods are not required to provide 100% coverage, but rather should be determined based on risk, criticality and security value."

Likes 0	

Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI’s comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	

Comment

Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, "access control" is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement "100 percent coverage is not required" is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement "as determined by the responsible entity." See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS that perform **authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS that perform **authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs).** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments. Please also see response to MRO's NSRF comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that "100 percent coverage is not required". The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of "networks" where there is no monitoring technology available. To address	

this concern, we suggest adding “routable protocol” prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Requirements

Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-

based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	

The intent does not seem to be reflected in what is written. The sentence, "100 percent coverage is not required" opens too many avenues for vastly different interpretations across industry. If the intent is for an entity to design how it will collect network data in a balanced manner with criticality in mind, then it should be stated. The "100 %" sentence could be replaced with, "Determine which CIP network communications are most critical to monitor. The monitoring and collection methods should provide security value to address the perceived risks."

Perhaps a different approach could be to clarify that the objective is not to monitor the endpoints. The language could state that 100% of monitoring endpoints in not required.

Likes 0	

Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

Comments: Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. **100 percent coverage is not required.** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 DT appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a “bump in the wire” tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do.

It is clear that 100% coverage isn’t required, but what provides “security value” and is considered “critical” isn’t. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.

Likes 0	
Dislikes 0	

Response
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.	
Likes 0	
Dislikes 0	

Response
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI’s comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a “bump in the wire” tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do.	

It is clear that 100% coverage isn't required, but what provides "security value" and is considered "critical" isn't. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	

While the current wording mentions that "100% coverage is not required", that leaves the possibility for an auditor to demand an arbitrary amount that is less than 100%. The SRC recommends adding verbiage indicating that the collection locations and methods should be commensurate to the risk posed as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike

Answer	No
Document Name	

Comment

Tacoma Power does not agree that the intent is clearly expressed in the language of Requirement 6 Part 6.1. The term "perceived risk" is not a well-defined or measurable quantify and as such, would be difficult to implement. There is no definition within the Requirement language

that clarifies what “internal” means in the internal network security monitoring term. Tacoma Power suggests defining internal network security monitoring. Tacoma Power suggests the following for the language of Requirement 6 Part 6.1: “Identify network data collection locations and methods that provide visibility of network communications (excluding serial) within the network subnets of applicable CIP Systems, to monitor and detect anomalous activity, including connections, devices, and network communications between applicable CIP Systems. Note: While complete coverage is not required, the implemented collection methods should increase the probability of detecting an attack that has bypassed network perimeter-based security controls.”	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	

Comment
The NAGF recommends that the SDT change Requirement 6.1 to state, “Identify network data collection location(s) and methods required to internally monitor applicable CIP networked environments that provide security value to address organizational risks.”

Likes 0	
Dislikes 0	

Response
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	

Comment
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP is concerned with the anticipated scope of Part 6.1 and believes the language should allow more flexibility for Responsible Entities to determine the network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity.

SPP proposes the following language for Part 6.1: Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous network activity indicative of an attack in progress.

Likes 0	

Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).

Likes 0	
Dislikes 0	

Response

Thank you. Please see response to ISO/RTO Council SRC’s comments.

James Keele - Entergy - 3

Answer	No

Document Name	
Comment	
The standard as drafted provides the latitude for entities to “identify network data collection locations and methods” as the first sentence of the question states. However, there is no identification in the standard of the expectations of entities to “perform an assessment” and “determine what is critical to monitor” as the second question of the sentence implies. If this is the expectation to assess and define, and entities will be audited against that assessment and definition, then it should be clearly detailed as an expectation in the standard.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	

The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. However the phrase ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. Suggest continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.	

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	

Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes the statement in the “Requirements” column of proposed Part 6.1, "100 percent coverage is not required," would almost certainly be both difficult to understand and difficult to audit. We note that the SDT addressed these concerns during the January 3, 2024

INSM webinar and provided a good explanation of what "percent coverage" was intended to mean (paraphrasing, a Responsible Entity's most important obligation is to design a collection system capable of detecting potentially malicious traffic on network segments between in-scope Cyber Assets, and so long as this is accomplished, it should be possible to justify not monitoring outbound and inbound traffic on every port on every device, which in some instances could be technically infeasible and/or prohibitively expensive). NST suggests either (a) deleting the "100 percent" statement, along with the one that follows ("Collection methods should provide security value to address the perceived risks.") or (b) moving them to the "Measures" Section of 6.1 if the SDT feels it is an important thing for Responsible Entities to understand.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

" EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that "100 percent coverage is not required". The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of "networks" where there is no monitoring technology available. To address this concern, we suggest adding "routable protocol" prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS devices that **perform access control functions** authenticate for other CIP Cyber Assets; **and**

{C}**2. PACS that rely upon EACMS that perform access control functions; and**

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS devices that authenticate for other CIP Cyber Assets; **and**

{C}**2. PACS that rely upon EACMS that perform access control functions; and**

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) **between applicable Cyber Assets** to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications. **100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.** "

Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement. In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT’s removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	

Dislikes 0	

Response
Thank you. Please see response to EEI's comments.
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment
SMUD proposes the following two options to improve Requirement R6 Part 6.1**:** "Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications, **as determined by the Responsible Entity**. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks." Or "**As determined by the Responsible Entity,** identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks."

Likes 0	
Dislikes 0	

Response
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing

the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The statement "100 percent coverage is not required." does not provide sufficient clarity on what, or how much must be collected. The next statement, "Collection methods should provide security value to address the perceived risks.", appears to try and qualify this, but still does not provide a sufficient guidepost for measuring compliance. Additionally, 'coverage' is not defined and further adds to the ambiguity.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.	

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Although NIPSCO agrees with the SDT’s intent, “100 percent coverage is not required,” seems ambiguous. This statement does not seem necessary in the language of the Standard as the Applicable Systems table defines the scope. This should be added to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the	

documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
The language in Part 6.1 is a rogue auditor's dream. If 100 percent is not required, then what percentage is acceptable and who gets to decide? If collection methods "should provide security value to address the perceived risks", then who gets to define "security value" or "perceived risks"?	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State agrees with MRO provided comments:

"The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome."

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the

documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	
Comment	

Oncor stands in agreement on the comments presented by EEI that states:

"EEI does not fully support the proposed language in Requirement R6, Part 6.1. Among our concerns is the statement that “100 percent coverage is not required”. While we appreciate the intent of this language, we feel it is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that simply identifying network communications may not be sufficient because there are types of “networks” where there is no monitoring technology available. To address this concern, we suggest adding “routable protocol” prior to network communications throughout R6. To address EEI’s concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**;

{C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**;

{C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network **communications**. **100 percent coverage is not required.** Collection locations and methods should provide security value to address the perceived risks**, as determined by the responsible entity**."

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being

developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

If a Responsible Entity (RE) is found non-compliant during an audit due to ambiguous and non-quantifiable standard language, the fines could result in money being spent paying a fine that would negatively impact security elsewhere through no fault of the RE.

"100 percent coverage is not required" is ambiguous, so compliance would be met if 99.9 % coverage were achieved, and it would also be achieved at 10% IF the collection methods provide security value to address the "perceived risks".

It doesn't matter if the RE has 100% coverage if the RE does not "perceive" any risk or does not know how it is defined or measured. Likewise, if the RE only has 10% coverage.

What is the intention of the regulation? A RE could log every single bit of every communication and alert on every single 'anomalous' behavior and if the RE is not "perceiving" a risk based on some objective measurement methodology or standard, the RE is neither reducing risk nor being compliant.

Since "perceived risks" does not appear to be in the NERC Glossary of Terms, how should it be defined, and whose, or what, perception is the standard by which the compliance is measured? By the RE's, the auditor's or the industry, or maybe it could be any of them? This should be better defined.

We do not provide any language modifications and recommend the SDT completely review this requirement part to develop minimum quantifiable measures for compliance and utilize existing glossary terms or develop glossary terms that can be used for this requirement.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

This requirement should be broken down into two parts. One for identifying applicable network communications, and the other for identifying monitoring methods.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing

the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	No
Document Name	
Comment	

Black Hills Corporation does not fully support the proposed language. Black Hills Corporation agrees with the comments provided by EEI, “EEI does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;
2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and
3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;

2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and

3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. *(remove "100 percent coverage is not required.")* Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**."

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the

documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

In response to industry comments regarding the applicability section, the Project 2023-03 DT unanimously determined that the record does not support inclusion of EACMS and PACs outside of the ESP. The drafting team has determined that the scope of the standard being developed should only include networks within each ESP. The DT's removal of EACMS and PACS outside of an ESP successfully resolves the concerns expressed by this comment. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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

PG&E does not believe the intent is clear for Part 6.1. PG&E recommends in addition to the "100 percent coverage not required", an additional clause be added that this should be a risk-based approach, as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO’s comments	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent.	

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA recognizes and appreciates the SDT’s effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors, which in this case could be about what percentage they cover and what they consider anomalous activity. BPA suggests that R6.1 be rewritten to more clearly specify the requirement, such as “Use a risk-based assessment methodology to identify	

network data collection locations…" Language used elsewhere in the CIP Standards, such as "as determined by the Registered Entity", could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc. BPA also suggests the final sentence ("100 percent coverage is not required…") could be incorporated into the Technical Rationale rather than the requirement.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
It is clear that 100% coverage isn't required, but what provides "security value" and is considered "critical" isn't. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements.	

It is clear that 100% coverage isn't required, but what provides "security value" is not. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard. Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase "based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
As written, R6 P1 is vague and will cause significant disagreement between entities as to what is considered sufficient "methods" to determine what must be collected. There is no existing standard within the cyber security practice on what precisely would constitute an effective level of data collection. While the drafting team states in the Technical Rationale that "Regional Entities would require too much INSM collection and force entities to move resources from other effective cybersecurity detection systems such as SIEM and endpoint	

monitoring to INSM collection", nothing about the standard itself places limits on interpretation by the RE such that what becomes deemed acceptable during audits is de facto direction by what the RE's want. For example, if during implementation it is determined that coverage of a selection of key devices is most appropriate and such selection of devices represents 75% of devices within a network because that is assessed to be the correct level of monitoring in a method, what constrains the RE from declaring the analysis to be insufficient?

In the Technical Rationale on page 8, it refers to examples of determining "assessment". However, the items listed as examples are not assessment tools to drive determination of what, precisely, should be collected at a per-packet level. Use of the MTIRE ATT&CK Framework is simply a taxonomy to "talk" about different stages of a cyber-attack and, notably, how to associate those terms with documentation. Two organizations using the ATT&CK framework will have substantively different interpretations of what a taxonomy element means and how it should be used, if at all. One entity's definition may not match an RE's definition and thus conflict will arise during audit. The Technical Rational does not solve interpretive differences, in fact it enhances them.

Another example of the problems with interpretation and execution is table of methods on pp 9-10 and combined with the reference diagram on page 14. The references are overly simplistic and not necessarily relatable to in-the-field deployments of network infrastructure. The "data collection" is referred to as a "TAP or SPAN" off a series of various switches or, in a few cases, "Network Flow". However, each label over-simplifies a significantly complicated series of engineering decisions. For example, most switches that are not large carrier-class devices, cannot effectively tap every single port and span/repeat those packets to another location. There are significant issues with processing power available on control planes of network devices, many of which will degrade the operational performance of devices if not carefully limited. Other proposed technologies, such as sFlow, are not security protocols. sFlow is, specifically, an industry protocol that was created to sample traffic moving through an interface for the purposes of calculating bust-based bandwidth billing (e.g., calculating the 95% percentile traffic for rate billing, etc.). The reference architecture also creates an interesting chicken-egg scenario, in combination with R6 P7, where monitoring assets will themselves become assets that require monitoring.
At the end of the day, the requirement and all associated rationale is very subjective and will lead to significant interpretive differences and clashes. If the SDT is not going to mandate 100% coverage – and all pervious CIP standards essentially require 100% coverage within a given set of "Applicable Systems" listed in the part – then the decision points need to be clear so that all entities can agree on reasonable interpretations of inclusivity within a defined set of boundaries.

Likes 0	

Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer	No
Document Name	

Comment

NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	

Comment

NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Even though the Requirement states "100 percent coverage is not required", this requirement is too subjective and open to different interpretations and implementations; this could prove difficult in providing adequate evidence in an audit. Suggested language for 6.1 is as follows: *"Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks."*	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent. Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
It is unclear what type of data is to be collected. Suggest revise to define expectations for what type of data should be collected. There is no minimum threshold for acceptable INSM coverage. Suggest revise to clearly define what type of data is to be collected, and establish a minimum threshold for what INSM coverage is acceptable. The undefined term “connection” is unclear in context. Suggest define what is meant by this term. Consider leveraging the OSI model to clearly identify the target depth of monitoring. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing	

the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
There are really two things being asked here: (1) perform the assessment to determine what is most critical to monitor and (2) identify the locations and methods to perform the monitoring. As written, it is not clear that both are being asked. So, this requirement either needs to be rewritten or broken up into two parts. It could be rewritten as “Assess network communications (excluding serial) between applicable Cyber Assets to determine the most critical communications and identify network data collection locations that monitor and detect for anomalous activity.”	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.	

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
The last sentence, which refers to security value to address the perceived risks, is highly vague. It is not clear how an auditor would verify what is the perception of risks for an entity or the security value.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Alison MacKellar - Constellation - 5	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the current language in 6.1 is clear to the intent that every network interface will not have to be monitored. Entities should consider however, that this approach will require they have a consistent rationale for what is included and be able to defend communications that fall into scope but were not selected for inclusion.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms.	

To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #4.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that under the current language 100 percent coverage is not required. Texas RE recommends, however, the language clarify and add threshold of acceptable monitoring so the standards applied and enforced consistently. Rather than mandating a specific minimum percentage, Texas RE suggests certain systems, such as operator consoles that are used to operate the Bulk Electric System, should be a mandatory inclusion within the INSM program. Alternatively, the SDT may wish to require entities to justify the parameters they have developed to meet the requirement to "[i]dentify network data collection locations and methods that provide visibility of network communications" so that the rationale for inclusion/exclusion is transparent.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing	

the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable. See additional comments for more details.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 Drafting Team (DT) appreciates the valuable feedback received regarding this question. There were numerous comments expressing support for providing flexibility to Responsibility Entities in determining the methods and locations for data collection, emphasizing the importance of a risk-based approach. However, concerns were raised regarding the usage of the phrase "100 percent coverage is not required" and certain other subjective terms. To address these concerns, the Project 2023-03 DT has made modifications to Requirement 1, Part 1.1 by removing the phrase "100 percent coverage is not required" and including the phrase “based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, guidance has been added to the measure for the	

documentation of the rationale for selecting or excluding monitoring locations. The Technical Rationale has also been revised based on industry feedback pertaining to this aspect of the requirement.

5. The Project 2023-03 SDT held extensive conversations about the term "baseline" and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT's use of the term "network communications 'baseline'" is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
The term baseline is appropriate because the entity is creating a baseline of the network activity, although there is room to improve the requirement. Consider rephrasing R6.3 to something like "Evaluate and create a network communications baseline using the collected data in Part 6.2." This should adequately differentiate this baseline from the one used in the CIP-010 standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	

The undefined term “baseline” is ambiguous, and is already in use in CIP-010 in a different context. Suggest revise to define what is meant by “baseline” in this context, preferably use a different term.

Identify clear retention requirements that are achievable with current marketplace offerings. For example, ISPs will leverage netflow data to maintain long term trends on interface and protocol utilization. It’s relatively low cost, and low storage requirements, yet allows for historical analysis and trending over time.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

As part of this goal to not inhibit usage of new technologies, the retention period and scope has been left at a high level such that the Responsible Entity can determine what is reasonable. The language “sufficient detail and duration to support analysis” in the current draft is intended to help support that not all data is required to be retained.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	

Comment

The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor

documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Suggested change: “network communication baseline” to “protocol baseline”. This aligns with the various ICS and non-ICS data communication protocols that could be detected in the network environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No

Document Name	
Comment	
Wording of 6.3, in particular, needs to be addressed by changing the word “Document” to “Establish” or “Develop” the expected network communication baseline. This will give the Responsible Entity the flexibility in their evaluation of the collected data in how they determine an expected network communication baseline.	
Likes 0	
Dislikes 0	
Response	
The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	

Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The use of “baseline”, while understandable, will still create overloading of the word as it’s already extensively used in CIP-010 and, by implicit reference, CIP-007 R1 and R2. Suggest the following language for Requirements: Record, evaluate and pattern the collected data sufficiently such that significant deviations from historical records are detectable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	

Comment
The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated. This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management. The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	

Comment
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network

traffic. This change supports the use of vendor proprietary technology for network traffic baselines, where the product may not be able to "output" a baseline but uses trending and comparisons to detect anomalies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes this requirement will be difficult to fulfill, as we don't know what a network communication "baseline" will look like. How do we document a baseline? It is also not sustainable to maintain a static documented baseline. PG&E believes this will most likely be defined by the security vendor that is being used and probably will not be publicly available (and will probably be internal configuration settings rather than a written baseline). PG&E also believes this requirement may not be feasible or necessary, given the logging and analysis requirements in other R6 sections**.**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	No
Document Name	
Comment	
Black Hills Corporation does not support the Requirement 6, 6.3 as currently written. Black Hills Corporation agrees with the comment provided by EEI, "EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** (*remove "Evaluate the collected data to document the expected"*) network communication baseline **through methods that record normal traffic to network assets and are continuously updated**."	

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

The term baseline can and will be confusing – since CIP-010 use the term “baseline”, There should be a different term to be used instead of using the term “network communications baseline”. The term ‘baseline’ already being widely used and understood across industry to refer to a software baseline in CIP-010 R1. Baseline is not sufficiently defined, and many would interpret this to imply a point in time capture of desired system state. The requirement states the baseline should be derived from evaluation of the collected data. However, collected data may differ considerably from the “Expected network communication” as documented in application/OS requirements and could lead to anomalous traffic being included within the baseline.

The recommendation would be to specifically define both “network communications baseline” and “software baseline” separately in the NERC glossary of terms.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance.

The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	No
Document Name	
Comment	
Oncor stands in agreement with comments made by by EEI that states: "EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a Evaluate the collected data to document the expected** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State agrees with MRO provided comments:

"The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3 and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish”. The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which is evaluates all network traffic."

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD recommends that the Standards Drafting Team simply remove the word “baseline” and we propose the following language for Requirement R6 Part 6.3.

“Implement methods to evaluate collected data to establish the expected network traffic.”

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
We agree that the concept of a network baseline makes sense but do have concerns that the diversity with which entities might construct these baselines . We support EEI proposed language to include “through methods that record normal traffic to network assets” at the end of 6.3 to encourage alignment on the expected outcome. It may be necessary to specify minimum elements for collection.If the term baseline is problematic, it could be removed all together in 6.3 if adequately specificity is given.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No

Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Richard Vendetti - NextEra Energy - 5	

Answer	No
Document Name	
Comment	

NEE supports EEI comments: " EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a Evaluate the collected data to document the expected network communication baseline **through methods that record normal traffic to network assets**. "

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term "baseline" into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term "baseline," as well as ensuring that the requirement does not unintentionally limit future technologies.

Jennifer Neville - Western Area Power Administration - 6

Answer	No
Document Name	
Comment	

Propose changing the term "document" to "establish." to enable demonstration that a baseline has been established, but not require documentation. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
It would be helpful to have particular aspects of a network communication baseline be clearly defined in the standard (similar to a baseline in CIP-010 R1.1). Maybe some wording like “including but not limited to”, so that utilities have some network communication baseline structure to work off of as recommended by NERC. This would clarify the compliance expectation when providing evidence for network communication baseline.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
James Keele - Entergy - 3	
Answer	No

Document Name	
Comment	
If the term “network communications baseline” is to remain undefined by NERC, then the requirement should include language directing the entity to define what constitutes the “expected network communication baseline” that is being documented and monitored. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. This ensures that monitoring and evaluation of deviations is occurring against a well-defined standard, and reduces compliance evaluation ambiguity for the entities both internally and externally.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP does not agree with the SDT’s use of the term “network communications baseline” in Part 6.3. With the industry-approved, virtualization-related changes from NERC Project 2016-02 including the removal of the term “baseline” from the currently enforceable version of CIP-010, the term “baseline” is not anticipated to be used in the future enforceable NERC CIP requirements. In addition, the SDT should consider adding “application flows” as part of the requirement language to help this requirement its overall intent. SPP proposes the following language for Part 6.3: *Evaluate the collected data to document the expected application flows and network communications.*	

SPP also supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No

Document Name	
Comment	
It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline. The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated. This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management. The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline. The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated. This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management. The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren would like more clarification around the term "baseline."	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
Avista agrees with EEI’s comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a Evaluate the collected data to document the expected** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	

Comment
From the NERC meeting which took place on 1/3/2024, the concept of a baseline was clarified to not be a point-in-time list, a spreadsheet, etc. but more of an expected network communication *behavior* and *functionality* against which the collected data can be evaluated. If this is the case, the Requirement should not have a term (baseline) that is to be interpreted. The focus is on evaluating expected network behavior against anomalous activities. Proposed language: “Evaluate the collected data to maintain the expected network behavior.”

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** network communication baseline **through methods that record normal traffic to network assets**.

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI’s comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance.	

The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
The term "Network communication 'baseline'" lacks clarity and introduces significant potential for confusion, particularly given its distinct usage in CIP-010. Consequently, it is advisable to refrain from employing "baseline" in the context of CIP-007 to avoid misinterpretation. The proposed Measures incorporate the term "expected network communications," which we believe adequately characterizes the information sought. However, the Measure itself falls short in delineating the specifics of the anticipated evidence. A record encompassing "expected network communications" is likely to amass a volume that surpasses human readability. This raises the pertinent question: What elements are anticipated to be included in this record? Does it necessitate an exhaustive enumeration of every conceivable endpoint and each individual protocol? Clarification is essential for a comprehensive understanding of the proposed Measure.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No

Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
More information is needed to determine what would be a suitable baseline. Does an entity have to provide documentation from vendors to support the baseline? Without more information on what constitutes a baseline and what evidence is required to justify the baseline it leaves too much open to interpretation by an auditor. Entities will vary on the methodology used to determine their baselines and this makes it hard for an auditor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. CEHE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. CEHE recommends revising the requirement to include a frequent evaluation of entities network	

communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company does not agree with R6 Part 6.3 as currently written. These requirement parts (6.2-6.5) are detailing a procedural “how” of meeting a security objective, which could be combined into “implement a process to monitor the identified collection points for anomalous activity including connections, devices, or communications” with response criteria and processes. A baseline can be a stated measure of how the entity determines anomalous activity. Southern Company suggests making the standard more future-proof, it needs to be more objective as security principles such as Zero Trust are incorporated with increasingly more communications in device to device encrypted tunnels thus reducing the usefulness of "on the wire" monitoring over time. Virtualization, containerization, micro-segmentation, etc. are all variables in how, and at what level, security monitoring may be best performed in the timeframe of this standard's implementation plan. Currently the language requires the baseline be built only from monitoring the network. We suggest the standard require what the entity is to accomplish, not procedural steps of how to “do” INSM with today’s tools. That is better left to Implementation Guidance or Technical Rationale and could simplify this requirement from its current 7 step process.	

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. SIGE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. SIGE recommends revising the requirement to include a frequent evaluation of entities network communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Considering the 2016-02 DT CIP-010 R1 language has moved away from documenting baselines and leveraging automation, the 2023-03 SDT should adopt a similar approach from - ‘Evaluate the collected data to document the expected network communication baseline.’ To - ‘Evaluate the collected data to establish the expected network communications.’	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
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 comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	

NST sees no problem with distinguishing network traffic baselines from endpoint device configuration baselines. We also note that if the most recent modifications to CIP-010 made by the Project 2016-02 SDT are approved by the NERC Board and by FERC, Responsible Entities will no longer be required to maintain configuration baselines as evidence of compliance with that Standard, which will further reduce the risk of confusion.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	

Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the use of the term “network communications baseline” in Requirement R6, sub-requirement 6.3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE agrees that network communications baseline is clear in Requirement R6 Part 6.3. If the SDT wishes to avoid the use of the word 'baseline' in this requirement Texas RE proposes any of the following requirement language alternatives:

- Evaluate the collected data to document the expected network communications profile.
- Evaluate the collected data to document the expected network communications traffic.
- Evaluate the collected data to document the expected network communications traffic pattern(s).

Likes 0	

Dislikes 0	

Response

Thank you for your comment. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one measure of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term "anomalous." The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of "anomalous" was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term "anomalous" was the appropriate term to use to describe that methodology. Do you agree that that the term "anomalous" effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word "anomalous" and phrase "indicative of an attack in progress." In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity's Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods "that provide value, based on the network security risk(s)." Third, the subsequent requirement is to "detect anomalous activity using the data collected at locations identified." The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
We understand the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated. Please see response to MRO’s NSRF comments.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Anomalous traffic may be expected from the baseline during outage or troubleshooting or testing, and it may be impossible to capture them in the network baseline. The standard should have verbiage to exclude those scenarios.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	

Answer	No
Document Name	
Comment	
AZPS believes that "anomalous activity" is ambiguous. We recommend language similar to the question above "deviations from a normal network communications baseline"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word "anomalous" and phrase "indicative of an attack in progress." In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity's Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods "that provide value, based on the network security risk(s)." Third, the subsequent requirement is to "detect anomalous activity using the data collected at locations identified." The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated. Please see response to MRO’s NSRF comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated. Please see response to MRO’s NSRF comments.	

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated. To the specific comment, it would be difficult to offer specific guidance on this scenario. For some entities, network traffic that looks like upgrades or testing could be malicious activity or an insider threat. The DT would recommend having processes in place at your entity to address those scenarios within the bounds of the requirements.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.

To the specific comment, it would be difficult to offer specific guidance on this scenario. For some entities, network traffic that looks like upgrades or testing could be malicious activity or an insider threat. The DT would recommend having processes in place at your entity to address those scenarios within the bounds of the requirements.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The term “anomalous,” is too vague and covers too many potential activities. The SRC recommends using the phrase from FERC Order No. 887: “anomalous network activity indicative of an attack in progress” as detailed below:

CIP-007-X Table R6 – INSM: Part 6.4 Requirements

*Deploy one or more method(s) to detect anomalous **network** activities **indicative of an attack in progress**, including connections, devices, and network communications using data from Part 6.2.*

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
While SPP does not have concern with the term “anomalous”, SPP believes the current purposed language is beyond the scope of FERC Order 887, which states “anomalous network activity indicative of an attack in progress.” SPP proposes updating the language in Parts 6.1, 6.4, 6.5, and 6.6 to include the language “anomalous network activity indicative of an attack in progress.”	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.
Bobbi Welch - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
If the term "anomalous" is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to "include criteria to evaluate and define attempts to compromise". If entities are allowed the latitude to define criteria for anomalous events to report to E-ISAC in CIP-008, they should be afforded that opportunity for anomalous events in this standard. This also reduces compliance evaluation ambiguity for the entities both internally and externally.	
Likes 0	
Dislikes 0	
Response	
The DT appreciates the feedback by Entergy. In the current draft, language has been added that may address this concern:	

"Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action."

Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to "anomalous network activity indicative of an attack in progress" should be subject to compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word "anomalous" and phrase "indicative of an attack in progress." In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity's Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods "that provide value, based on the network security risk(s)." Third, the subsequent requirement is to "detect anomalous activity using the data collected at locations identified." The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	

Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends where possible align proposed terms with NIST current definitions. NIST definition examples: Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences. Behavioral Anomaly Detection - A mechanism providing a multifaceted approach to detecting cybersecurity attacks.	
Likes 0	
Dislikes 0	
Response	
The DT appreciates the feedback from Reclamation and will take it under advisement.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No

Document Name	
Comment	
While Dominion Energy understands why the term "anomalous" was chosen by the SDT, we recommend additional clarifying language be added to make it clear that stakeholders, who have the best understading of their networks, are responsible for determing what is anomalous. We recommend the addition of the phrase "as determind by the Registered Entity" be added to qualify anamolous.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State recoomends using the words normal or abnormal in place of anomalous.	
Likes 0	
Dislikes 0	
Response	

The DT appreciates the feedback by Tri-State and will take it under advisement.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
The recommendation would be not to use the word “anomalous” at all. Recommend the use of “unusual communications that need to be investigated” instead. Using the terms “unusual communications that need to be investigated” removes the ambiguity of what an entity would define as “anomalous”. If the word “anomalous” is used in the standard, it must be defined in the glossary of terms with the definition specific to the SDT’s intent of its definition, namely, “unusual communications that need to be investigated” since the dictionary definition of the word anomalous is, “deviating from what is standard, normal, or expected.” This definition would allow for entities to consider an “unusual communications that need to be investigated” event as “normal” or “expected” and the expected understanding of the word anomalous in this context and requirement would be lost.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	

The DT did discuss the creation of defined terms, but it resulted in conflicts with currently enforceable standards or other drafts currently in development, and so the decision was made to not pursue that currently.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The term “anomalous” is too broad. We suggest focusing on wording similar to “deviations from the network communications baseline.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
DT should consider defining anomalous to avoid any confusion for entities. See additional comments for more details.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated. The DT did discuss the creation of defined terms, but it resulted in conflicts with currently enforceable standards or other drafts currently in development, and so the decision was made to not pursue that currently.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes the term “anomalous” is vague. PG&E recommends using the phrasing from FERC Order 887 “anomalous network activity indicative of an attack in progress.”	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO’s comments	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Manitoba Hydro understands the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of	

an attack in progress" should be subject to compliance. This clearly defines the scope of the standard, for example if a product detects anomalies related to system network communication malfunctions these may be useful to an entity but out of scope of compliance. Leaving the term "anomalous" in continues to differentiate between detected "anomalous" activity and a confirmed attack in progress.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word "anomalous" and phrase "indicative of an attack in progress." In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity's Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods "that provide value, based on the network security risk(s)." Third, the subsequent requirement is to "detect anomalous activity using the data collected at locations identified." The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The use of "anomalous" is fine however suggest including "potentially" and to align with proposed language from proposed R6P2: Deploy one or more method(s) to detect potentially anomalous activities, including connections, devices, and network communications using data from Part 6.2	
Likes 0	
Dislikes 0	
Response	

The DT appreciates the feedback from FirstEnergy and will take it under advisement.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
MRO NSRF understands the reasons presented for using the term "anomalous," but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term "anomalous network activity indicative of an attack in progress" used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to "anomalous network activity indicative of an attack in progress" should be subject to compliance.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The undefined term “anomalous” is ambiguous and may create confusion for both entities and the CEA to determine what specific activities are included. Suggest revise to provide a clear criteria for determining what activities are “anomalous” that is consistent with existing CIP-008 obligations.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.

The DT did discuss the creation of defined terms, but it resulted in conflicts with currently enforceable standards or other drafts currently in development, and so the decision was made to not pursue that currently.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
The term “anomalous” is not specific enough. It would be clearer to build on the language used in R6.3. In R6.3, we essentially determine what is not “anomalous” (e.g., what is acceptably part of the network communications baseline). Consider rephrasing as “to detect activity that deviate from the network communications baseline identified in Part 6.2” or similar. This clarifies the intent, eliminates the need to include “anomalous”, enhances cybersecurity by converting the “black list” to a “white list” monitoring method, and reinforces the importance of the communications baseline throughout R6.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has had numerous discussions on vetting the usage of, and alternatives to, the word “anomalous” and phrase “indicative of an attack in progress.” In the current draft of the requirements, we believe that several changes may help address concerns about scope. First, the scope of the requirements has been reduced to applicable systems within the Responsible Entity’s Electronic Security Perimeters. Second, language was added to the draft for identifying collection locations and methods “that provide value, based on the network security risk(s).” Third, the subsequent requirement is to “detect anomalous activity using the data collected at locations identified.” The DT believes that this will allow entities flexibility, but also helps to create bounds on what data needs to be collected and evaluated.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	

Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	

See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is of the opinion that the term "anomalous" is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI is of the opinion that the term "anomalous" is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with use of the term “anomalous”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes

Document Name	
Comment	
One potential issue NST does see here arises from the DT's assertion, in the draft Technical Rationale document, that a baseline is "Continuously updated by a computer" and not a "Point-in-time list." We believe these assertions are incorrect. Merriam-Webster's online dictionary defines "baseline" as, "a usually initial set of critical observations or data used for comparison or a control." Similarly, several references NST consulted define network baselines as "snapshots" that can be used to set expectations about traffic types, volumes, sending and receiving devices, etc. during some period of time (e.g., weekdays from 8 AM to 6 PM local time). While we certainly agree baselines should be updated periodically, we are hard-pressed to understand how anomalous traffic can be detected if a baseline that is intended to represent "expected" traffic is being ***continuously*** updated.	
Likes 0	
Dislikes 0	
Response	
We are assuming that this comment is in response to Question 5. The DT has moved the term “baseline” into the Measures section for the current draft. The requirement language is now focused on methods to detect anomalous network activity, with documenting a baseline being one of several example measures of compliance. The DT believes that this will alleviate concerns or confusion around the term “baseline,” as well as ensuring that the requirement does not unintentionally limit future technologies.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies. “	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the term "anomalous" is appropriate.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
It would be clearer to use language in R6.5 like that of CIP-005-7 R1.5 "Have one or more methods". Also, as stated in question 6, not using the term "anomalous" would be beneficial here. Consider language like "Have one or more method(s) to evaluate activity that deviates from the baseline identified in Part 6.2." This approach supports the ability to evaluate the finding before initiating a CIP-008 Cyber Security Incident determination while maintaining continuity with other existing standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and created CIP-015-1 Requirement R1, Part R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The word anomalous was removed from the section. The DT believes the change satisfies the concern of the comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	

The undefined term “anomalous” lacks the clarity to distinguish between activities addressed in Part 6.4 and activities that should initiate a CIP-008 process.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The word anomalous was removed from the section. The DT believes the change satisfies the concern of the comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Constantin Chitescu - Ontario Power Generation Inc. – 5	
Answer	No

Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
As above, suggest the inclusion of "potentially" and to outline that anomalous may not be malicious: One or more process(es) to evaluate potentially anomalous activity identified in Part 6.4 to determine appropriate action including, but not limited to, adjustments to the traffic patterns from Part 6.2 or investigation as a potential security incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The word anomalous was removed from the section; however, the intent of R1 is, "…To improve the probability of detecting anomalous or unauthorized network activity." Accordingly, the addition of the word "potentially" is not warranted to qualify "anomalous". Additionally, Page 4 of the Technical Rationale	

states, “Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity’s ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint.” In turn, this allows entities to determine which anomalous activity is determined to be malicious or innocuous. The DT believes the changes satisfy the concern of the comments.	
Jeffrey Streifling - NB Power Corporation – 1	
Answer	No
Document Name	
Comment	
It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough. There is no wording stating specifically that escalation and potential initiation of a responsible entity’s CIP-008 process is the appropriate action if a legitimate threat is detected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	

It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. To clarify the link the requirement could be re-worded:

One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine if it is related to a Cyber Security Incident.

The measures lists potential evidence as “documentation of responses to detected anomalies”. Manitoba Hydro suggests removing this from the measures to focus on evidence related to having the process documented. When systems are first put in they may generate a lot of alerts before they are “tuned” and evidence of review of every single alert may be burdensome without any practical security value.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT revised the measures to include, but not limited evidence to:

- Detection events;
- Configuration settings of INSM monitoring systems; or
- Documentation of a baseline used to monitor against unauthorized network activity.

The DT believes the change satisfies the concern of the comments.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE recommends the following requirement language: One or more process(es) to evaluate anomalous activity identified in Part 6.4 as a potential Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
It is not clear how to determine when action is required.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
I believe this question may refer to an older version of the draft standard. This question makes more sense regarding Part 6.5, and the INSM drafting team outreach presentation discusses CIP-008 in the context of Part 6.5. However, the actual language of Part 6.5 does not reference CIP-008, and therefore any anomalous activity could be interpreted as an attempt to compromise and/or an actual compromise that triggers the requirements of CIP-008. It isn't enough to include the SDT's intention in an outreach presentation - if it isn't in the standard, an auditor will not consider it.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No

Document Name	
Comment	
This question appears to reference CIP-007-X Requirement R6 Part6.5 and this question is not clear and not very well defined. We recommend changing Requirement R6 Part 6.5 to state: “Implement methods to evaluate anomalous activity identified in Part 6.4.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
In 6.5 Duke Energy recommends additional language to clarify the intent of the evaluation. *One or more process(es) to evaluate anomalous activity identified in Part 6.4 for indications of an attack in progress, and if such indications are detected, to determine appropriate action.*	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO’s NSRF comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As currently written, neither R6 nor any of its parts say anything about CIP-008. NST suggests language such as, "Develop and deploy methods to detect anomalous network activity and to identify potential Cyber Security Incidents."	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends adding additional language to CIP-007 R6 to clarify that this occurs before the determination of a Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Suggest including language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vise versa.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The language wasn’t that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change provides clarity.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	

Since the requirement language in R6 Part 6.5 does not mention CIP-008 or Cyber Security Incidents, there is no relationship established between R6 Part 6.5 and CIP-008 or a Cyber Security Incident. Additionally, the requirement language may fall within the current processes identified for Cyber Security Incident Response by the Responsible Entity, and could cause multiple response paths to be created.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to "identified". It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough. There is no wording stating specifically that escalation and potential initiation of a responsible entity's CIP-008 process is the appropriate action if a legitimate threat is detected.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The language wasn’t that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to “identified”. It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.	

There is no wording stating specifically that escalation and potential initiation of a responsible entity's CIP-008 process is the appropriate action if a legitimate threat is detected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
As written, the requirement could potentially result in a self-report if any “anomalous activity” occurs and is not detected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	

Comment	
The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO’s NSRF comments.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

The use of the term “anomalous’ in Requirement R6, Part 6.4 is fine, but this starts to overlap with an entity’s CIP-008 Incident Response Program”. An entity already has definitions for attempt to compromise in the Incident Response Plan and if “anomalous” activity is detected it should refer back to its incident response plan. Just because an entity detects anomalous activity and they refer to their incident response plan it does not mean it is a Cyber Security Incident, it just needs to be investigated.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not believe that Requirement R6, Part 6.4 nor Requirement R6, Part 6.5 addresses the process of evaluating anomalous activity prior to escalation and potential initiation of a responsible entity’s CIP-008 process. Requirement R6, Part 6.4 requires methods to detect anomalous activity. Requirement R6, Part 6.4 does not address investigation or evaluation. Requirement R6, Part 6.5 requires a process to evaluate the anomalous activity identified in Requirement R6, Part 6.4. SIGE suggests including “prior to the initiation of a responsible entity’s CIP-008 process” in Part 6.5 so that the new requirement would read, “One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action, prior to the initiation of a responsible entity’s CIP-008 process.”	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests that clear language be added to tie R6.5 and/or R6.6 to CIP-008 in coordination with the Project 2022-05 drafting team. How a hand-off from a suspected malicious event is directed into a reporting requirement for "attempts to compromise" is under discussion under Project 2022-05. Ambiguity around analyzing whether an event is a security incident, what threshold for reporting such an incident might need, and the process to tie it into incident response activities including mitigation has the potential for creating duplicative and distracting	

requirements. BPA recommends the SDT change the word “Deploy” to “Utilize”. BPA believes deployment implies implementation of new technologies not currently in the Registered Entity’s environment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 DT was clear that Part 6.4 would occur before determining if a Cyber Security Incident had occurred.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	

Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear."	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Alison MacKellar - Constellation - 5	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

SPP agrees that the process to determine appropriate action regarding anomalous activity in Part 6.4 occurs prior to escalation and potential initiation of a Responsible Entity's CIP-008 process (i.e., before the determination of a Cyber Security Incident). However, there appears to be a typographical error in this question. SPP believes the SDT intended to reference Part 6.5 since it is more appropriate for the content of this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, "Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action." The words "anomalous" and "baseline" were removed from the section. The DT believes the change satisfies the concern of the comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF believes that the process has been adequately clarified.	
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 agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The process is clear as laid out in 6.4 detection and 6.5 evaluation. It is only this question that is confusing, referencing only 6.4 in a discussion about the 6.5 evaluation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The Project 2023-03 DT vetted the issues and revised CIP-015 R1.3 (formerly CIP-007 R6.5) to, “Implement one or more process(es)method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.” The words “anomalous” and “baseline” were removed from the section. The DT believes the change satisfies the concern of the comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you. Please see response to EEI's comments.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	

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	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes outlined in Question #5 (above).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response in Question 5.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE believes that the requirement itself is objective- based; however, the scope described in the CIP-007-X Technical Rationale is in broad prescriptive terms. The Technical Rationale should clearly state that it does not determine the scope.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Scope of the current draft Standard has been reduced as suggested.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
There doesn't appear to be much latitude in how to implement methodology.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While the implementation does require network collection and analysis, the TR has been updated to reflect a more acceptable method of analysis and to ensure that various tools can be used to comply with the standard.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC believes requirement part 6.3, which mandates the evaluation of collected data to document the expected network communication baseline, poses a limitation on certain technology platforms, notably Intrusion Detection Systems (IDS). This constraint arises from the inherent characteristics of certain IDS technologies, which may not facilitate the documentation of an expected network communication baseline. In specific instances, certain IDS technologies generate alerts predicated on Indicators of Compromise (IoC) signatures without establishing a network model for triggering alerts based on anomalous behavior against the established network communication model.	

The FERC order specifically identifies IDS as a potential technology for implementing Internal Network Security Monitoring.

In Part 6.1, GSOC recommends aligning the use of terms like "Cyber Asset" in Requirement language with the terminology used in the recently approved versions of the Standard drafted by Project 2016-02. Specifically, in that version of the Standard, the coverage would only extend to a physical Cyber Asset, overlooking a Virtual Cyber Asset.

In Part 6.1, the exclusion labeled "(excluding serial)" lacks clarity, especially when contemplating the utilization of serial-based network communications like T1's. GSOC suggests refining this exemption to enhance clarity, citing other instances in the Standards where exclusions for this type of communication are present or possibly utilizing routable communications.

In Part 6.2, GSOC finds it unclear what type of log data is required and the necessary retention policy to comply with the current wording. GSOC proposes incorporating objective language that allows entities to define an appropriate retention period for the log data.

Concerning Part 6.3, GSOC notes that the Requirement lacks sufficient clarity regarding what constitutes an evaluation. It merely states that the entity should look for deviations from expected network communications without specifying what should be included in expected communications.

GSOC suggests that Part 6.4 could potentially be combined with 6.3, and perhaps even 6.5, for enhanced clarity.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Based on comments received, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. The context of CIP-007-X, Requirement R6, Part 6.2 is now revised and is within Requirement R3 of CIP-015-1: “R3. Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.”

The Technical Rationale was updated per this comment to reflect that many methods of detection are acceptable. IDS was specifically added as an acceptable detection method to the Technical Rationale. Note the caveat in the Technical Rationale that historical/traditional IDS systems do not retain a record of network traffic which is required in Requirement R3. Some current IDS systems do retain network

communications data which could meet the intent of Requirement R3. Note that order 887 identifies IDS as “some of the tools” and specifically calls IDS multipurpose. As such, an IDS could be a component of an INSM system, but more likely is one component of an INSM system. Order 887 also identifies anti-malware and firewalls in the same location as IDS, but it is clear that none of those technologies by themselves are sufficient to meet the intent of the order. IDS signatures are very good at detecting known attacks, but have proven historically to be less competent at detecting unknown attacks. In the TR, IDS is identified as a legitimate component of an INSM system, and entities are encouraged to use IDS, but an IDS system would likely need to be combined with other tools in order to create a compliant INSM system. Note also that the more modern IDS technologies such as Suricata have additional logging features that can be utilized in an INSM system and note that modern IDS technologies such as Suricata are frequently combined with other tools such as zeek, in order to develop a detection system that has broad detection capabilities. Part 6.2 (now R3) clarifies in the Technical Rationale document the log data and allows the Responsible Entity to determine retention policy with guidelines suggested in the Technical Rationale. We believe this achieves what you suggested. Part 6.3 was removed, and baseline/anomaly detection was clarified in the Technical Rationale to be one of several options for detection technologies (along with IDS). Part 6.4 was combined with parts removed.

Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Although R6.4 allows the latitude for various INSM Methodologies and technologies; it also must satisfy R6.1. Hence, R6.1 should be defined in more detail. See response to Q4 above.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The DT revised Requirement R6, Part 6.1 and 6.4 (from CIP-007-X) when creating CIP-015-1, Requirement R1 and its part to provide clarity to addresses this comment.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
There doesn’t appear to be much latitude in how to implement methodology.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While the implementation does require network collection and analysis, the Technical Rationale has been updated to reflect additional methods of analysis and to ensure that various tools can be used to comply with the standard.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you. Please see response to EEI's comments.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	
Tacoma Power does not agree that the Table R6 requirements allow latitude for various INSM methodologies. The NSM process described in R6 is one way to solve the Internal Network Security Monitoring Order, but other methodologies exist to gather and alert on malicious internal East/West traffic. It may be beneficial to recast the entirety of R6 in the Risk Mitigation ideal to mitigate the risk posed by malicious network activity within the CIP-Networked Environment. Part 6.2 should include "per system capability" to ensure that entities are not required to collect data on systems that may not have the capability.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While the implementation does require network collection and analysis, the technical rationale has been updated to reflect additional methods of analysis and to ensure that various tools can be used to comply with the standard. CIP-015-1, Requirement R1, Part 1.1 allows Responsible Entities the ability to collect data in a way that can monitor systems that may not have a built-in capability. Note that network data must be collected, but the language allows Responsible Entities and vendors wide latitude to collect necessary data.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	

Comment	
SPP does not agree the SDT was successful in creating an objective-based approach, particularly with the concerns expressed in SPP's comments for questions 4, 5, 6, 9, and 11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to comments in Questions 4, 5, 6, 9, and 11.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy greatly appreciates the work of the drafting team to create INSM requirements while trying to balance the need for flexible language. We are concerned that that the draft requirement allows too much latitude and will result in significant differences between INSM programs from responsible entity to responsible entity.	
Likes 0	
Dislikes 0	
Response	
Several other comments state that there is not enough latitude. It's not a problem to have significant differences between INSM programs – in some ways that would make it harder for adversaries to successfully attack multiple utilities without being detected.	

In response to this comment, the DT created Draft 1 of CIP-015-1. Please see substantial updates to the Technical Rationale document, which could help align INSM programs across the industry: “The entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.”	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
Based on the technical rational and the various diagrams that have been presented, SMUD believes that the INSM requirements are both prescriptive and subjective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
A 'No' response is based on ambiguities but agree that latitude is allowed for various INSM methodologies and technologies to be used now and in the future.	

Likes 0	
Dislikes 0	
Response	
In response to this comment the DT re-drafted CIP-015-1. Please see substantial updates to the Technical Rationale document which could help reduce ambiguity.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E believes some of the requirements need additional clarification, as noted in our earlier comments.	
Likes 0	
Dislikes 0	
Response	
In response to this comment the DT re-drafted CIP-015-1. Please see substantial updates to the Technical Rationale document which clarify many of the requirements.	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on	

certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
This standard is very clear that an ISNM system is not automatically designated as EACMS. As stated in the Technical Rationale document, INSM systems are a poor choice for monitoring electronic access to an EAP because an INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems that are very accurate at detecting failed or successful logons. If a Responsible Entity uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is probably a legitimate designation for that entity. A Responsible Entity that can monitor electronic access using other tools would not need to designate their INSM as EACMS. The CIP-015-1 standard leaves that designation up to each Responsible Entity.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not find that R6 Part 1 is objective or will lead to objective outcomes. Please see comments above.	
Likes 0	

Dislikes 0	
Response	
In response to this comment the DT re-drafted CIP-015-1. Please see substantial updates to the Technical Rationale document.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Consider leveraging the OSI model to clearly identify the target depth of monitoring and retention. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.	
Likes 0	
Dislikes 0	
Response	

The DT drafted some concepts that use the OSI model, but did not require collection at a specific level of the OSI model. In some situations it may make sense for an entity to avoid specific traffic. In the current draft CIP-015-1, the decision is left to each Responsible Entity and the OSI model may be a legitimate way for the Responsible Entity to demonstrate compliance with Requirement R1, Part 1.1. The updated Technical Rationale document has an expanded section under Requirement R3 that outlines many levels of data collection that could be included in the retained data. The Responsible Entity may determine what is required based on their risk assessments or other criteria.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
We agree that Requirement R6, as written, provides latitude for various methodologies and technologies to be used. However, the broadness and ambiguity of some of the requirements and measures may lead to disagreements between entities and auditors that sufficient monitoring and documentation have been provided. Without providing more specific guidance on the type of information that should be	

available within data logs, retention periods, response timelines, and assessments of anomalous activities, this could lead to auditors issuing PNCs for an entity where they deem that the documentation being provided as evidence is insufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. In response to this comment the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document which could help reduce ambiguity.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Project 2023-03 SDT did create a requirement that was objective based and allowed latitude for various INSM methodologies, but this is a double-edged sword, with the large amount of latitude it leaves too much varying interpretations between what an auditor is expecting, and an entity is doing. In addition, there will be varying ways in which entities across different regions meet this requirement some will go above and beyond while others do the bare minimum which again leaves it up to an auditor if enough is being done to be compliant.	
Likes 0	
Dislikes 0	
Response	
In response to this comment the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document which could help reduce ambiguity. The DT declined to make specific recommendations and minimum requirements, due to the large number of potential combinations of INSM methodologies.	
Robert Blackney - Edison International - Southern California Edison Company - 1	

Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above.	
Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT drafted CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic	

access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining "electronic access monitoring" as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT drafted CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	

We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining "electronic access monitoring" as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
This standard is very clear that an ISNM system is not automatically designated as EACMS. As stated in the Technical Rationale document, INSM systems are a poor choice for monitoring electronic access to an EAP because an INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems that are very accurate at detecting failed or successful logons. If a Responsible Entity uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is probably a legitimate designation for that entity. A Responsible Entity can monitor electronic access using other tools.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF believes that the proposed Requirement R6 is objective based and will allow for various INSM methodologies and technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
This effort and work to meet the requirements and allow flexibility in execution of the requirements is greatly appreciated.	

Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above."	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you – please note the DT created CIP-015-1. Please see substantial updates to the Technical Rationale document also.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees the language in Requirement R6 is objective and allows latitude, noting our proposed changes above.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support. Please see responses to proposed changes above.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes

Document Name	
Comment	
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	
Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

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

Answer	No
Document Name	

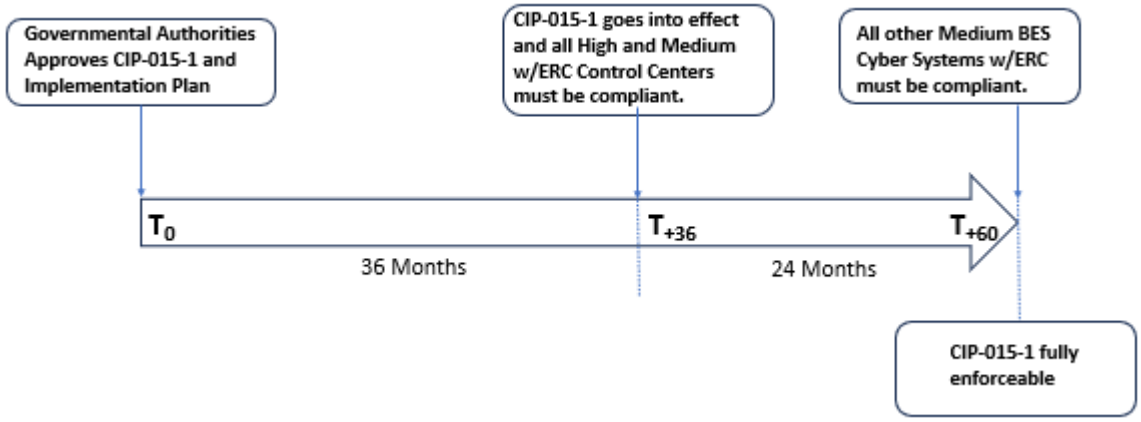
Comment

The ambiguity with the proposed language makes it difficult to assess implementation timeframes.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT added a graph to help clarify the implementation timeframes.



Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	
Comment	

MRO NSRF appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document.

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	

With the increased concern of critical infrastructure infiltration by foreign adversaries, 36 months should be applied to all systems inside and outside of Control Centers. This should be conceivable since Part 6.1 provides latitude to not having 100% coverage of network data collection locations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
36 months for Control Centers and 60 months for applicable systems located outside Control Centers should be sufficient only if the language in Part 6.1 of “100 percent coverage is not required” is updated with the following (or similar): *“Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.”*	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Without clear expectations of the Drafting Team toward the Industry Members, we cannot support the implementation Plan of CIP-007-x.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In March 2022, BPA made the following comment in response to FERC's INSM NOPR: *"Bonneville estimates implementation timelines for INSM on High Impact BES Cyber Systems alone to be around three to five years. If entities are also required to adopt INSM on Medium Impact BES Cyber Systems with ERC, it would likely take on the longer end of that timeline to implement.* After reviewing the new requirement language in R6, BPA believes more time will be required to implement an INSM program. This takes into consideration the effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No

Document Name	
Comment	

Manitoba Hydro appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. The 36 month timeline may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document.

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

Answer	No
Document Name	
Comment	

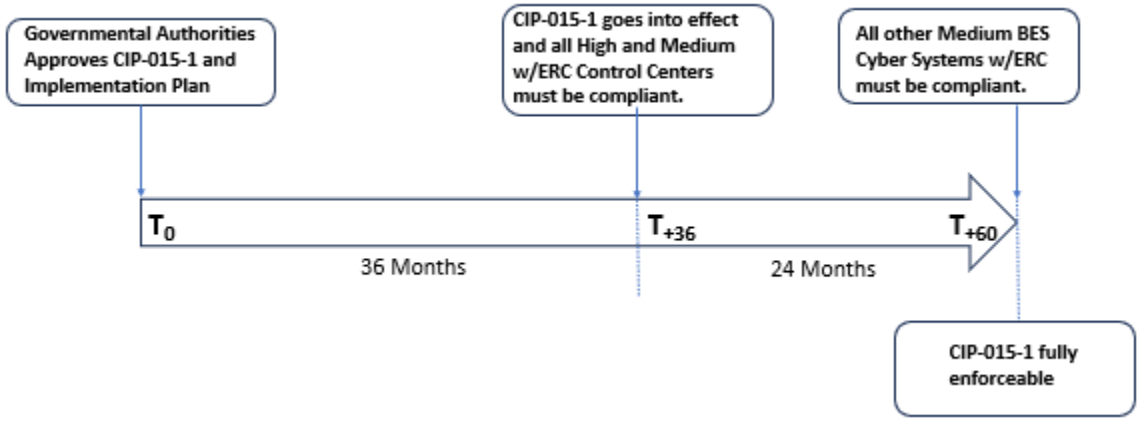
Dominion Energy has concern over the 36 month implementation due to supply chain concerns. Dominion Energy requestis 48 months for Control Center and keep 60 months for the other applicable systems not located at Control Centers.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

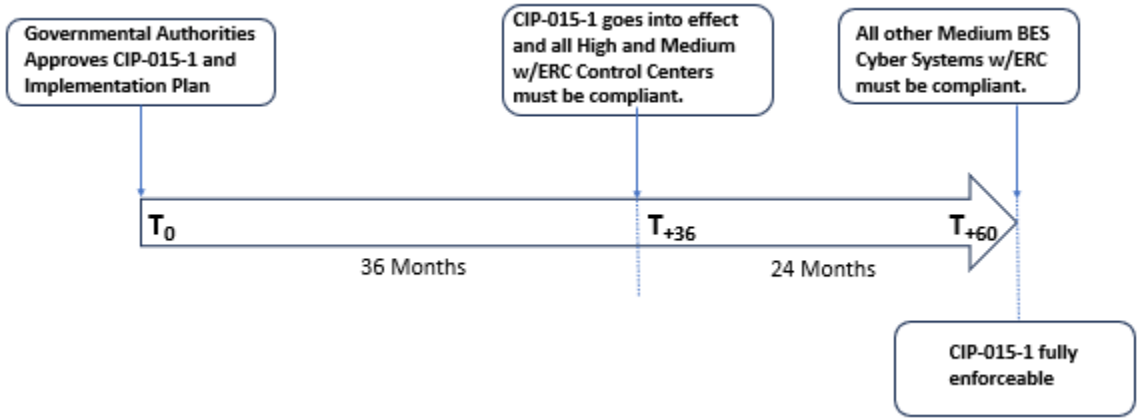
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree with the proposed schedule.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. EACMs and PACs outside of the ESP are not requirements for CIP-015-1.	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Unknown if 36 months is sufficient for implementation - it depends on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. Further, the Technical Rationale on pg. 4 should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1, removing the “100 percent coverage is not required,” and has updated the Technical Rationale document. The DT made modifications to CIP-015, Requirement R1, Part 1.1 by removing the phrase, "100 percent coverage is not required," and including the phrase, “Based on the network security risk(s).” This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, the DT added guidance to the measure for the	

documentation of the rationale for selecting or excluding monitoring locations. Moreover, the DT revised the Technical Rationale based on industry feedback pertaining to this aspect of the requirement.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
There could be cases where entities may not be able to procure, test, configure, and fully deploy an INSM solution within the stated months. A suggestion is to allow each entity to respond with an appropriate timeframe for implementation that is viable to it. The Regional Entity can be afforded oversight to their entities' commitment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP does not agree with the Implementation Plan for Draft 1 of proposed CIP-007-X based on the concerns expressed in SPP's comments for questions 4, 5, 6, 9, and 11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. Please see responses to SPP's comments in Questions 4, 5, 6, 9, and 11.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT added a graph to help clarify the implementation timeframes. 	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

If the FERC Order involves monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC finds the provided timeframe sufficient. Nevertheless, due to the ongoing lack of clarity in the scope, it is challenging for us to provide comments, resulting in a “No” response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT added a graph to help clarify the implementation timeframes.	



Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in order to ensure communications is not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

Likes 0	
Dislikes 0	

Response
Thank you for your comments. This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
We appreciate the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control

system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents." This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1, removing the "100 percent coverage is not required," and has updated the Technical Rationale document. The DT made modifications to CIP-015, Requirement R1, Part 1.1 by removing the phrase, "100 percent coverage is not required," and including the phrase, "Based on the network security risk(s)." This change allows for the implementation of risk-based approaches in collecting data for INSM without being prescriptive. Additionally, the DT added guidance to the measure for the documentation of the rationale for selecting or excluding monitoring locations. Moreover, the DT revised the Technical Rationale based on industry feedback pertaining to this aspect of the requirement.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation supports the proposed Implementation Plan, but 36 months would be the minimum time required to implement. Black Hills Corporation also agrees with the proposed changes from EEI, "EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see Page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below). ***(remove "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.")***	

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. Please see response to EEI’s comments.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	

Oncor stands in agreement with comments presented by EEI that states:

"EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging."

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. Please see response to EEI's comments.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports the proposed Implementation Plan and the phased approach.

Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below). **Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.** Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging. "	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document. Please see response to EEI's comments.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	

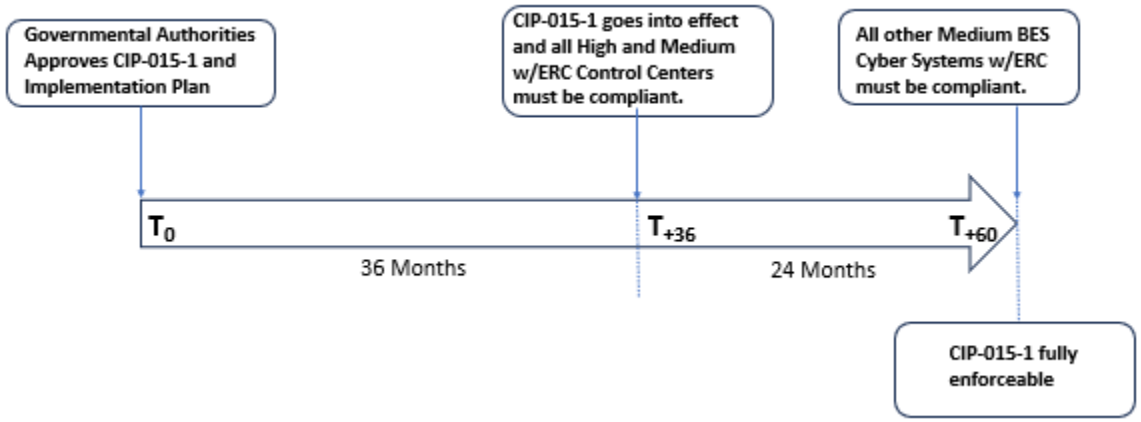
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF supports the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
The implementation plan could clarify these timelines better and how they stack. Currently it is not obvious.	
Likes 0	

Dislikes 0	

Response

Thank you for your comment. The DT added a graph to help clarify the implementation timeframes.



Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	

Comment

Avista agrees with EEI's comments and recommendation for Technical Rationale:

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Remove the following:

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment

capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Insert the Following:

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Thank you. Please see response to EEI's comments. The DT has created CIP-015-1 and updated the Technical Rationale document:

"Vendor Constraints

Some ICS vendors have historically stated that their systems do not support cybersecurity monitoring using either INSM data collection or endpoint logging collection. Rather than add a "per system capability" exclusion, Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and data collection methods appropriate to each entity's ESP networks."

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

Answer	Yes
Document Name	

Comment

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document:

"Vendor Constraints

Some ICS vendors have historically stated that their systems do not support cybersecurity monitoring using either INSM data collection or endpoint logging collection. Rather than add a "per system capability" exclusion, Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and data collection methods appropriate to each entity's ESP networks."

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	Yes
Document Name	

Comment

ITC supports the response submitted by EEI.

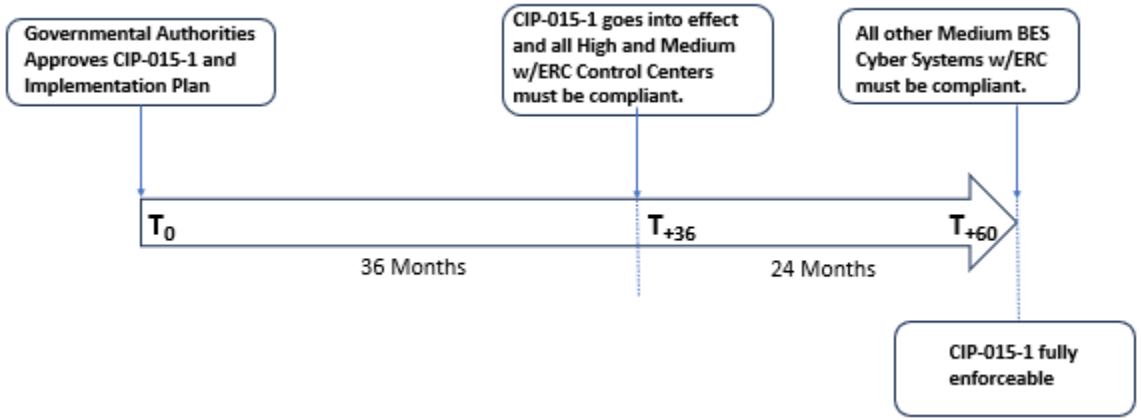
Likes 0	
Dislikes 0	

Response

Thank you. Please see response to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with EEI's comments and recommendation for Technical Rationale:	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes

Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
3 years for Control Centers and 5 years for non-control centers is acceptable but more technical guidance or requirement clarity is required to meet auditors' expectations. The technical rational and guidance need more clarity to align the auditors and implementors.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT has created CIP-015-1 and updated the Technical Rationale document to provide additional clarity and guidance.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

Yes, however the more time the better some entities will already have upgrades planned and this will have to be figured into the upgrades.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the implementation duration. However, Southern Company would offer the suggestion to have separate sentences with "…the standard shall become effective for Control Centers on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees". "…the standard shall become effective for medium impact BES Cyber Systems with ERC not located at Control Centers on the first day of the first calendar quarter that is sixty (60) months after the date the standard is adopted by the NERC Board of Trustees". We believe this would help with confusion that is occurring with the Implementation Plan as currently written.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT added a graph to help clarify the implementation timeframes.	



Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	

Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joshua London - Eversource Energy - 1, Group Name Eversource	

Answer	
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
Developing and maintaining the necessary processes and procedures to maintain a sufficient level of documentation for compliance purposes will create a need for entities to increase the number of FTEs. We have already seen an increase in costs associated with INSM from vendors over that past few years and expect that once this requirement is approved, costs will increase further due to the limited number of vendors with applicable OT solutions.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. While the DT has no control over vendors, the DT believes the removal of EACMS and PACs outside the ESP helps to resolve some of the economic concerns expressed by this comment.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp – 6	
Answer	No
Document Name	
Comment	

May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and for CIP-015 R1.1 (formerly CIP-007 R6.1), the language changed to, “…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications.” The DT revised language on Page 4 of the Technical Rationale to provide entities a, “…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity’s ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint.” The DT believes the changes resolve the concerns expressed by this comment.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It will take an untold number of man-hours to

evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
It is Southern Company's opinion that the cost effectiveness of the current proposed requirements can vary greatly depending on what percentage below 100% in R6.1 is determined to be compliant in each region, and what specific Cyber Assets are determined to require monitoring. In addition, there are significant concerns about supply chain constraints given a limited pool of Operational Technology (OT) vendors with INSM products.	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Cost effectiveness is difficult to judge with the first draft. Ultimately cost effectiveness will be determined by the final draft. Additional oversite and help may be required for compliance.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No

Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
If the scope of the FERC Order requires monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC contends that cost-effective solutions can achieve this goal. However, there is ambiguity in interpreting how to manage EACMS and PACS INSM data. In instances where these Cyber Assets might exist outside the ESP, it becomes unclear how much equipment would be necessary to retrofit existing infrastructures.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	

Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

The new requirement is inherently not cost effective.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option	

to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	

The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	No
Document Name	
Comment	
Tacoma Power needs additional clarity to understand the scope of work and boundaries of what's covered in this Standard in order to assess cost.	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 DT vetted these issues. Industry comments centered around concern of EACMS and PACs outside the ESP, CIP-015 R1.1 (formerly CIP-007 R6.1) not requiring "100% coverage", and costs. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No

Document Name	
Comment	
The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks the SDT to consider the potential cost that may arise from the scope of this requirement. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, and storing of all data between every cyber assets within an ESP, for any length of time, will be substantial. Not all network architectures are created equal and could be more costly and time consuming to implement for some Responsible Entities than others. Virtualization of network, server, and storage infrastructure, and the complexity it	

brings to the table, has the potentiality to make packet captures, baselining of traffic, monitoring, analyzing, and alerting much more difficult if a Responsible Entity is unable to obtain visibility into all of the network traffic within a subnet.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
It is not clear that all sub parts of requirement R6 could be cost effective. It is a new requirement that would mandate an entity to effectively not only procure a brand new solution, but produce an entirely new process and procedures, in addition to the human resources and associated roles and responsibilities, with which the entity must comply. Although it's possible certain entities would not have a financial burden for this kind of expenditure, it may be a significant burden for others.	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Jennifer Neville - Western Area Power Administration – 6	
Answer	No
Document Name	
Comment	
The cost effectiveness is dependent upon updating the language to 6.1 regarding "100 percent coverage is not required." Per response to Q4 this should be removed and replaced by continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity." If Part 6.1 governs costs could be contained to a reasonable amount. Further, the Technical Rationale on pg. 4 should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option	

to gather cybersecurity information at the network or endpoint." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree the proposed changes are cost-effective.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
This inclusion of cyber assets outside of High BCS and Medium BCS with ERC is not the most cost-effective approach to increasing the security posture of those cyber assets. Addressing boundary-level (north-south) controls for these assets would be more cost-effective approach and a logical first step to creating a common understanding of a "trust zone" for these device types before an east-west monitoring construct is applied.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT believes these changes provide the means to resolve many of the concerns expressed by this comment.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD feels that the determination of cost effectiveness varies based on the methodology used, but prescribing network communication baselines as the methodology would not be cost effective.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	

Comment	
NIPSCO has not determined whether R6 will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	
Likes 0	
Dislikes 0	

Response	
The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	

Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	

Comment	
The expansion of the scope of the FERC Order to include PCA, EACMS, and PACS will significantly increase the implementation costs. Although the standards drafting team indicated that assets not currently in scope of the CIP standards are not included (for example, Corporate AD servers that are not currently EACMS), it is likely that audit teams will have different interpretations.	
Likes 0	

Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Not too sure what the exact cost will be for each entity, but the cost of monitoring can be a costly endeavor for many entities, including SRP.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 DT vetted these issues. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option

to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E cannot determine if the modifications are cost effective at this time. There are still unknowns as to the required scope (% coverage) and data retention requirements. We would like to see more industry feedback before deciding.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
May or may not be cost effective depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to Q4 this should be removed and replaced by continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity." If Part 6.1 governs costs could be contained to a reasonable amount. The problem is with the Technical Rationale regarding Vendor Support on p. 4: "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents." This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware may not be cost effective.	
Likes 0	

Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.

Jeffrey Streifling - NB Power Corporation - 1

Answer	No
Document Name	

Comment

There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's

ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This change in the standard will result in significant resource expenditure, including wholesale replacement/architecture of existing networks, that will be exceptionally costly and such costs will be passed on. Implementing this standard will result in the potential of hundreds of network devices all requiring replacement with devices that are significantly more costly simply to add the ability to execute some form of intra-lan monitoring. Additionally, the potential reliability impact of requiring major network architecture needed is much higher than modest security gains.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to,	

"Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC's comments.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Depending on if the language in Part 6.1 is updated, this may or may not be cost effective. If the language of "100 percent coverage is not required" is updated with language similar to the following: *"Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks."*, then the implementation plan should be sufficient as proposed by the SDT.	
Likes 0	
Dislikes 0	

Response
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	

Comment
May or may not be cost effective depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to Q4 this should be removed and replaced by continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity." If Part 6.1 governs costs could be contained to a reasonable amount. The problem is with the Technical Rationale regarding Vendor Support on p. 4: "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents." This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace "may need to" with "could" and should add alternative options regarding monitoring workarounds. Retrofitting "outdated" hardware may not be cost effective.

Likes 0	

Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.

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

Answer	No
Document Name	

Comment

The ambiguity with the proposed language makes it difficult to assess implementation cost.

Likes 0	
Dislikes 0	

Response

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the

word “baseline” and instead drafted for CIP-015 R1.2, “Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1.” CIP-015 R1.4 language further reduced the burden on log retention by changing to, “Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3.” The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree and disagree. Since the standard allows the latitude, cost effective solutions can be implemented but will it be good enough to meet the auditor’s expectations? The technical rational and guidance need more clarity to align auditors and implementors.	
Likes 0	
Dislikes 0	
Response	

The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the	

data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.	
Likes 0	
Dislikes 0	
Response	
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	

Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to IRC SRC's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	

Response
The Project 2023-03 DT vetted these issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve the concerns expressed by this comment.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	

Response
Thank you. Please see response to EEI's comments.

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to ISO/RTO Council SRC's comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Byron Booker - Oncor Electric Delivery - 1	
Answer	
Document Name	
Comment	
Oncor will not submit comments on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	

Comment
BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.

Likes 0	
Dislikes 0	

Response
The Project 2023-03 DT vetted these cost-effectiveness issues and worked to provide more clarity around these concerns. The DT agreed the standard does not support inclusion of EACMS and PACs outside of the ESP, which reduces the economic impact to industry. Additionally, DT revised the CIP-015 R1.1 (formerly CIP-007 R6.1) language to, "…Methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications." Further, the DT revised language on Page 4 of the Technical Rationale to provide entities a, "…Wide latitude to identify INSM data collection locations and design data collection methods appropriate to each entity's ESP networks and allows vendors the option to gather cybersecurity information at the network or endpoint." The DT removed the use of the word "baseline" and instead drafted for CIP-015 R1.2, "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1." CIP-015 R1.4 language further reduced the burden on log retention by changing to, "Implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3." The DT believes these changes provide the means to resolve many of the cost concerns expressed by this comment.

11. Please provide any additional comments for the SDT to consider, if desired.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
Data retention requirements are ambiguous and subject to interpretation by entities and the CEA. Suggest revise to provide guidance regarding retention requirements by data type.	
Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
MRO NSRF appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot. For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please	

explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Regarding CIP-008, MRO NSRF urges the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point.

Lastly, MRO NSRF thanks the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.

Likes 0	
Dislikes 0	

Response	
In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Whereas CIP-012 communications are between ESPs and are not in scope. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Regarding CIP-008 comment this was included as a Measure for R1.3.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	
Document Name	
Comment	
For Part 6.5, reword sentence to begin, “Develop one or more process(es)…” For Part 6.7, reword sentence to begin, “Develop one or more process(es)…”	
Likes 0	
Dislikes 0	
Response	
Thank you. The DT developed CIP-015-1 and revised requirement and requirement part language.	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	

Dislikes 0	
Response	
Thank you.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC’s comments.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	
Document Name	
Comment	

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a device to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful

authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS. INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS. The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.	
Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 DT provided a response to question 8, and for your reference, please refer to the following: This standard is very clear that an ISNM system is not automatically designated as EACMS. An INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems that are very accurate at detecting failed or successful logons. If a Responsible Entity uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is probably a legitimate designation for that entity. An RE that can monitor electronic access using other tools would not need to designate their INSM as EACMS. The CIP-015-1 standard leaves that designation up to the capable people at each Responsible Entity.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

BPA recommends adding language addressing the intended periodicity or ongoing nature of the proposed R6 Parts. BPA can't determine based on the proposed requirement language how often the ERO-Enterprise (ERO-E) would expect entities to perform the location identification, data logging, and baselining requirements. In order to avoid inconsistent interpretations among Registered Entities and auditors across the ERO-E, BPA recommends the SDT include language in the requirements that specifies a minimum cadence by which the aforementioned tasks should be completed or that clarifies the RE is empowered to determine the cadence. The SDT should clarify if the intent is to have methods and processes for R6.4 through R6.6 that address patterns of behavior and processes to analyze them, rather than isolated pieces of traffic.

BPA also recommends adding minimum log retention timeframes as a compliance metric and to align with other CIP standards. R6.7 should be modified to cover risk of data exploitation as follows: "…protect the data collected in Part 6.2 to mitigate the risks of exploitation, deletion, or modification by an adversary…"

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines.

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	
Document Name	

Comment

Manitoba Hydro appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and

limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. The term "adversary" has been removed.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	

Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 appreciates the effort the DT had taken in creating a Standard to meet FERCs Order with a very aggressive time frame. PG&E will be waiting to see the next version of these requirements based on our and other Registered Entities feedback that include the scope and percentage of coverage of Cyber Assets**.**	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
Section 4 comment: The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable to 6.1. The entity should also consider documenting the reasons why others were not considered critical.	

Stating "100 percent coverage is not required" can lead the entities to only monitor a few CIP network interfaces without any clear direction to comply with the standard, and not use this opportunity for the intent purpose of the standard to monitor and protect the internal networks from security threats.

Section 6 comment: Per the information gathered from CIP-007-X, the use of word “anomalous” doesn’t clearly indicate the use of both network baseline and the signature-based tools to identify anomalous. E.g., 6.4 states “Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2” which could lead entities to use only log collected data and not network baselines indicated in 6.3 to detect anomalous (including malicious) activities.

Additionally, SDT should consider defining anomalous to avoid any confusion for entities.

Additional Comment

There is no requirement to reevaluate the environment after changes or on a periodic basis to ensure that the entity is monitoring the higher risk traffic.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has created CIP-015. For the "100 percent coverage is not required" please refer to the Measures for Requirement R1, Part 1.1 that gives additional guidance, as this phase has been removed from the standard. Project 2023-03 DT does not agree that anomalous needs to be defined.

Kimberly Turco - Constellation - 6

Answer	
Document Name	

Comment

Constellation has no additional comments.

Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
It appears by the name of the R6 table, Internal Network Security Monitoring, the intent of this requirement is to monitor internal network traffic. However, this intent is not present in the requirement language. For example, Requirement R6 Part 6.1 states that communications between applicable Cyber Assets are in scope. High impact BCS are in scope, as are medium impact BCS with External Routable Connectivity. These BCS are commonly found in discrete networks, however the requirement language does not clearly exclude from scope communications between these applicable systems found in discrete networks. If the SDT intends for communications between Applicable Systems in discrete networks to be in scope, then no change is needed. If the SDT does not intend for communications between Applicable Systems in discrete networks to be in scope, Texas RE recommends modifying the requirement language to convey this.	
Likes 0	
Dislikes 0	

Response	
In response to industry comments, the Project 2023-03 DT has updated the language accordingly within a new proposed CIP-015 standard and newly proposed three requirements. The Table format has been removed due to the precise language for the Applicable Systems column.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	
Document Name	
Comment	
Oncor stands in agreement withg the comments being submitted by EEI that states: **"BCSI Implications (NEW Proposed)** For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for	

cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

(NEW Proposed) EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. Suggest either deleting this phrase or changing it to “detecting attacks that may bypass electronic security perimeters”.

EEI suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.

(**NEW Proposed**) EEI additionally suggests the following boldface edits (below) for Requirement 6, part 6.5 to make it clearer the expectation that entities have when they are evaluating anomalous activity.

6.5 One or more process(es) to evaluate anomalous activity identified in Part 6.4 **and to determine appropriate action which include a process for:**

6.5.1: Identifying an attack in progress and actions to be taken in response; and

6.5.2 Evaluating anomalous activities and actions to be taken in response."

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has updated the language accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Cloud-based service for INSM is an option for the Responsible Entity. Based upon the Responsible Entity's evaluation criteria the INSM solution can either be BCSI designation stored location or an EACMS. This is up to the Responsible Entity to decide, and Project 2023-03 DT wanted to give the Responsible Entity options to consider for the designation of INSM solution.

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	

Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	
Document Name	
Comment	
If the scope of this proposed standard was limited to the scope of the FERC Order (assets within the Electronic Security Perimeter), then this standard language should be part of CIP-005, not CIP-007.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Mark Flanary - Midwest Reliability Organization - 10	

Answer	
Document Name	
Comment	

1. Part 6.5 language is inconsistent with the other R6 sub-parts. All others start with an action verb. We suggest updating 6.5 to begin as "Evaluate anomalous activity...". The process language is inherited from the higher-level R6 requirement language.

2. Part 6.7 - Same statement as for Part 6.5 - We suggest beginning it with "Protect the data collected..."

Likes 0	
Dislikes 0	
Response	

In response to industry comments, the Project 2023-03 DT has updated the language accordingly.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	
Document Name	
Comment	

SMUD appreciates the Standard Drafting Team's effort to revise CIP-007-X to include INSM requirements, but we have the following additional recommendations:

- Move Requirement R6 Part 6.4 (deploy) so that it is before Part 6.2 (log). Part 6.4 should become Part 6.2, then Part 6.2 will then become 6.3, and Part 6.3 will become Part 6.4 with all other parts staying where they are;

- Move all INSM requirements and parts to CIP-005; and

- In the Applicable Systems column, just state EACMS and/or PACS. Do not add where they perform access control functions. There are no other CIP requirements that state anything other than EACMS and/or PACS.	
Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 DT has updated the language accordingly within a new proposed CIP-015 standard and newly proposed three requirements. The Table format has been removed due to the precise language for the Applicable Systems column.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	

Duke Energy thanks the Drafting Team for their work to thoughtfully address FERC Order 887. There are some additional items that we would like to recommend to add clarity to the INSM revisions.

- Duke Energy recommends Requirement 6.1 is updated to require entities to specify the types of data to be collected in their documented processes, so that the data that will be expected for part 6.2 is clearly tied back to part 6.1.
- Additionally, use of the same phrase “network data” in 6.1 and 6.2 would bring greater clarity to the requirements, updating 6.2 to read “Log collected network data at the network locations identified in Part 6.1.”
- We also request clarity on the use of the term “connections” in 6.1. Does this intend to refer to TCP/UDP “connections” or the connecting and disconnecting of devices to network switches or some other definition of this term? Alternative language such as “monitor and detect anomalous activity, including the presence of anomalous devices in the network and use of anomalous communication protocols in the network” would provide a clearer requirement.
- Duke Energy also recommends that the INSM requirements are moved to their own Standard outside of CIP-007. CIP-007’s traditional focus on device-level security controls is at odds with the broader subject matter of network monitoring, and following the model used by CIP-012 for a new subject matter with no current analogous scoping would facilitate the introduction of this technology and scope, as well as lay the groundwork for elimination of duplicate requirement language in CIP-007 and CIP-003 if Low applicability later added.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	
Document Name	
Comment	

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add "as determined by the documented processes or procedures of the Responsible Entity."

Similar to above, suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Whereas CIP-012 communications are between ESPs and are not in scope. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

Thank you. Please see response to MRO's NSRF comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	

NEE agrees with two of EEI additional comments:

"EEI is concerned that in Requirement R6, the phrase "that has bypassed other security controls" is too broad and generic of an objective statement as there are attacks that may bypass "security controls", such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to "that has bypassed other electronic security controls".

EEI suggested adding "in Part 6.2" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity. "

"Data Collection Methods, Pages 9 through 10

The term "CIP-networked environment" is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment."

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST believes it would be helpful for R6 Part 6.6 to identify a minimum retention period for INSM data unless the SDT intends for it to be the standard 3-year period defined in Section C Part 1.2 ("Evidence Retention"). The language in the proposed Measure for 6.6, "...with data retention configuration with timelines sufficient to perform the analysis of anomalous activity" is vague and could easily be subject to a considerable number of widely different interpretations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines.	
Alison MacKellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has no additional comments	

Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	
Document Name	
Comment	
In Part 6.2, the measure describes an example evidence, which is the data collected. It is not clear why the focus is on the data collected and not the configuration of logging the data, which is the actual stated requirement. Observation: CIP-007 R6 applicability assumes all assets are known and classified according to CIP-002 and only requires baselining of network traffic between applicable assets. But if an unknown malicious device is put on the network, because it is unclassified and not a BCA, PCA, EACMS, or PACS, and is on its own interface, the entity does not have to pay attention to it or its anomalies. Example – if someone installs a rogue device on the network that initiates a portscan, the entity does not have to recognize the device or the portscan as a network baseline deviation. Along those lines, because TCAs are excluded from applicability, the entity does not have to pay attention to TCAs even though their insertion on the network at odd hours may be anomalous. The structure allows the entity to entirely ignore rogue devices as an attack vector.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are	

still in scope and should be considered during any INSM implementation. Furthermore, this will include TCA while they are temporarily connected within the ESP.

Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	

Comment

SPP would like the SDT to consider the following:

Comment for Part 6.2:

SPP is concerned with the requirement language for Part 6.2. The proposed language is open to interpretation and could significantly impact the cost of storage as well as create compliance risk. What needs to be logged? How should the log be evidenced? Is a summary sufficient? How long do the logs need to be retained?

Comment for Part 6.4:

The proposed language for Part 6.4 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.4:

Using the data collected pursuant to Part 6.2, deploy one or more method(s) to detect anomalous network activity indicative of an attack in progress.

Comment for Part 6.5:

SPP suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

SPP proposes the following language for Part 6.4:

One or more method(s) to evaluate the anomalous network activity indicative of an attack in progress identified in Part 6.4 and determine appropriate action.

Comment for Part 6.6:

The proposed language for Part 6.6 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.6:

One or more method(s) to investigate anomalous network activity indicative of an attack in progress.

Comment for Part 6.7:

SPP does not agree with using the term “adversary” in a NERC requirement due to its ambiguity. SPP also suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.
The term "adversary" has been removed.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	

Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike	
Answer	
Document Name	
Comment	
TPWR believes that the INSM Requirements fit better in CIP-005, due to the Purpose statement found in the latest CIP-005-8: "To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).", **than in CIP-007 which contains the Purpose** "To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)." The Title of CIP-005 may be due for an update as well, since the Title remains "Electronic Security Perimeter(s)" which is no longer fully inclusive of all that CIP-005 includes. One option for the Title of CIP-005 would simply be "Network Security." Tacoma Power offers this language for the high level R6:	

"Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-XXX-X Table RX – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed network perimeter-based security controls."

Tacoma Power believes that the requirement language provided does not align with the scope of monitoring identified in the Webinar on the slide titled 'Interpretation of the Term "CIP Networked Environment"'. Specifically, many of the red "out-of-scope" network paths are not out of scope based on the requirement language. Specifically between the EACMS/EAP and the EACMS Access Control and the EACSM/Intermediate System. EACMS/EAPs and EACMS/IS both perform access control functions and are therefore specifically included in scope. Additionally there are a significant number of additional "in-scope" network paths that are not clarified on the diagram, since the diagram only includes a single ESP and the current language does not limit the scope to the networks associated to each individual Applicable System.

Editorial Comments on Section 3, Purpose:

- The purpose statement should include the acronym after "BES Cyber Systems", as follows:

"To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems **(BCS)** against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

Editorial Comments on Section 4, Applicability:

- The term "Special Protection System" and "SPS" should be deleted throughout Section 4.
- Regarding Bullet 4.2.3.5: delete "-5.1" from CIP-002-5.1. The bullet should read "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the **CIP-002** identification and categorization processes."
- The following exemption is missing and should be added as Bullet 4.2.3.3: "4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations."
- Bullet 4.3 is missing. Recommend adding this bullet, as follows: "4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies."
- Bullets 4.2.3.1 and 4.2.3.2 should refer to "Cyber Systems" and not "Cyber Assets"

Editorial comments on Table R6:

- In the "Applicable Systems" column, the word "impact" should not be capitalized. Additionally, the acronym "BCS" should be used instead of "BES Cyber System" and "ERC" instead of "External Routable Connectivity." Example of how this should be written: "Medium **impact BCS** with **ERC** and their associated…"

Comments related to alignment with Project 2016-02, CIP Virtualization:

- The title of CIP-007 Table R1 should be changed from "Ports and Services" to "System Hardening" to align with the Project 2016-02 changes. The title of Table R1 should also be changed in the R1 language.
- The title of CIP-007 Table R2 should be changed to "Cyber Security Patch Management" to align with Project 2016-02.
- The language in the following Requirement Tables in the CIP-007 redline do not match the changes in Project 2016-02. Tacoma Power recommends updating these tables to align with the recent CIP-007 draft in Project 2016-02.
- Table R1: Part 1.1 and Part 1.2 need to be updated. Part 1.3 is missing from Table R1.
- Table R2: Parts 2.1 through 2.4 need to be updated.
- Table R3: Parts 3.1 through 3.3 need to be updated.
- Table R4: Parts 4.1 through 4.4 need to be updated.
- Table R5: Parts 5.1 through 5.7 need to be updated.
- The Violation Severity Levels table should also be updated to align with the Project 2016-02 changes.
- Table R6, Parts 6.1 through 6.7 should include this statement at the end of the Applicable Systems list: "SCI supporting an Applicable System in this Part."

Other Editorial Comments:

- "C. Regional Variances" should be "D. Regional Variances"
- The Section E, Interpretations, is missing. Recommend adding this section.
- "D. Associated Documents" should be "F. Associated Documents".

Likes 0	
Dislikes 0	
Response	

The Project 2023-03 DT has created CIP-015 and revised previous Requirement R6 and its parts. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	
Document Name	
Comment	
The SRC notes that Parts 6.5 and 6.7 use different phrasing than the remaining parts of Requirement R6, and recommends that Parts 6.5 and 6.7 be revised to begin with "Implement one or more process(es)..." to better align with the language used in the rest of Requirement R6.	
Likes 0	
Dislikes 0	
Response	
Thank you. The DT developed CIP-015-1 and revised requirement and requirement part language.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1. Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.	

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has the Responsible Entity determine what criteria is used to define baseline and in turn what are the anticipated and tolerated deviations. This has moved to Measure 1, Part 1.2. The DT has created CIP-015 standard and revised the requirements from the previous Requirement R6 and its parts.

This standard is very clear that an ISNM system is not automatically designated as EACMS.

An INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems that are very accurate at detecting failed or successful logons.

If a Responsible Entity uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is probably a legitimate designation for that entity.

A Responsible Entity that can monitor electronic access using other tools would not need to designate their INSM as EACMS. The CIP-015-1 standard leaves that designation up to each Responsible Entity.

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	
Document Name	
Comment	

It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1.

Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber

System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has the Responsible Entity determine what criteria is used to define baseline and in turn what are the anticipated and tolerated deviations. This has moved to Measure 1, Part 1.2. The DT has created CIP-015 standard and revised the requirements from the previous Requirement R6 and its parts.

This standard is very clear that an ISNM system is not automatically designated as EACMS.

An INSM system cannot accurately determine if a login was successful or failed for encrypted protocols. A better choice would be SIEM or log monitoring systems that are very accurate at detecting failed or successful logons.

If an RE uses an INSM as the only system capable of monitoring electronic access to a BCA, then EACMS is probably a legitimate designation for that entity.

A Responsible Entity that can monitor electronic access using other tools would not need to designate their INSM as EACMS. The CIP-015-1 standard leaves that designation up to each Responsible Entity.

David Jendras Sr - Ameren - Ameren Services - 3

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	
Document Name	
Comment	
Avista agrees with EEI's comment: EEI suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below) Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	
Document Name	
Comment	

It is unclear why the SDT did not incorporate the proposed CIP-007 R6 Requirement into already existing Standards. Logging and log evaluations could have been added to CIP-007 R4, and malicious/anomalous activity capturing and evaluation could have been added to CIP-007 R3.

With regards to CIP-007-X R6.3, if an entity were to add a new system into its environment, how long would it have to be compliant with creating a new baseline? This is not clear in the proposed Requirement.

CIP-007-X R6.6 states, “Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.” What constitutes “sufficient detail and duration”, and how would that be audited?

Likes 0	
Dislikes 0	
Response	

In response to industry comments, the Project 2023-03 DT has updated the language accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines.

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to “that has bypassed other electronic security controls”.

EEI suggested adding “in Part 6.2” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.

Technical Rationale Comments

BCSI Implications (see Classification Rationale, Page 3)

For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

Data Collection Methods, Pages 9 through 10

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 DT has updated the language accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Cloud-based service for INSM is an option for the Responsible Entity. Based upon the Responsible Entity's evaluation criteria, the INSM solution can either be BCSI designation stored location or an EACMS. This is up to the Responsible Entity to decide, and Project 2023-03 DT wanted to give the Responsible Entity options to consider for the designation of INSM solution. The Technical Rationale has been updated so that Responsible Entities can evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement INSM.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
We support additional commentary as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI’s comments. Please also see responses to MRO’s NSRF comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	

Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
Avista agrees with EEI's comment: Comments: EEI suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below) Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	
Document Name	
Comment	

In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the of the SDT:

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network.
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0	
Dislikes 0	

Response

Thank you for your comment. In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines. The term baseline has been moved to Requirement R1, Part 1.2 measures so the Responsible Entity can determine what criteria is used to define this term.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	
Document Name	

Comment

The technical rational and guidance need more clarity to align auditors and implementors.

INSM system will have to meet the definition of EACMS as it performs electronic access monitoring function. It is unclear why there was an option not to classify it as EACMS but only BCSI. Clarity is required.	
Likes 0	
Dislikes 0	
Response	
Thank you. The DT developed CIP-015-1 and revised requirement and requirement part language.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
Part 6.6 necessitates an explicit definition of data retention requirements. The current specification, which mandates retention with "sufficient detail and duration to support the investigation of anomalous activity," introduces a potential challenge. The determination of what constitutes sufficient detail and the appropriate duration is contingent upon the detection and subsequent investigation of anomalous activity. This approach poses a risk of non-compliance in scenarios where anomalous activity is identified after the data has been discarded. To mitigate this risk, it is advisable to allow for flexibility in retention periods, tailored to the specific nature of the data. For instance, considering the substantial volume of packet captures, it may not be pragmatic to retain them for extended periods. A more nuanced approach that accommodates variations in retention periods for different types of data would enhance practicality and adherence. We recommend consolidating the proposed Requirements into one or two cohesive Requirements. Additionally, GSOC believes that addressing this requirement within the framework of CIP-005 may be a viable and more streamlined alternative. This consolidation and alignment could contribute to a more coherent and manageable regulatory framework	
Likes 0	

Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its own analysis to provide sufficient timelines. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements.

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	
Document Name	

Comment

In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the SDT:

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network?
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Project 2023-03 DT has left this up to the Responsible Entity to determine retention process(es) based upon its

own analysis to provide sufficient timelines. The term baseline has been moved to R 1.2 measures so the Responsible Entity can determine what criteria is used to define this term.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO's NSRF comments.	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
There are some concerns about CIP-007-X R6.3, how often does an entity analyze the traffic? Is it weekly, monthly, or would an instant alert be required. Without a little more direction an auditor and entity may disagree on the frequency.	
Likes 0	
Dislikes 0	
Response	
Thank you. The DT developed CIP-015-1 and revised requirement and requirement part language.	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rationale document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. CEHE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.	
Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 DT updated the Technical Rationale so that Responsible Entities can evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement INSM.	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	
Document Name	
Comment	
Scope of Requirement Parts: The SDT has a diagram of many EACMS and PACS communications with various forms of communication either in or out of scope represented by blue/red arrows. Southern Company suggests the diagram is not clearly represented in the requirement part scope language. For example, the diagram says the communications within a PACS out to its controllers is not in scope, however the requirement scope only states that PACS are in scope (those that rely upon an EACMS for access control). Once a PACS meets that condition,	

then the entirety of the PACS is in scope, which includes its distributed controllers as the requirement part itself explicitly says "between applicable Cyber Assets" within these systems (the PACS definition only excludes the badge readers, etc. at individual doors). That could be hundreds of widely distributed controllers across the enterprise in scope of this INSM requirement because the PACS is in scope and the main sentence of the requirement is written to "visibility between all applicable Cyber Asset" level, not the system level. There are huge implications of the Cyber Asset granularity rather than monitoring the communications to/from the PACS as a singular system. The SDT diagram is based on communications between systems, but the scoping of the requirement is visibility of all the applicable Cyber Assets within those systems and thus all communications to or from each individual programmable electronic device are in scope. While it states 100% is not required, it seems it is then left as an exercise to the entity to prove why they do not monitor 100% if they only monitor the PACS database server for example. This construct is quite prone to differences of opinion and perceived risk in audits.

As another example, only EACMS that perform access control functions are in scope, but once in scope, then the visibility of all communications between all of its applicable Cyber Assets are in scope, thus all the arrows to any such EACMS are included. The scoping in the standard tells the entity what systems are in scope, but then its focus is monitoring the networks on which those systems reside which will include all comms to/from those systems. It is unclear in the scoping language how that allows for the red "out of scope" arrows.

Southern Company suggests that the requirements be left at the BCS, EACMS, and PACS level, without mention of Cyber Asset within the requirement part language, which would more clearly allow entities the flexibility to monitor to the level of granularity within these systems that provides monitoring value commensurate with the expense and reliability impact of individual components. In the PACS example, the greatest security monitoring value may be for the database server containing the access rights database, but little value in monitoring hundreds of distributed controllers controlling individual doors in facilities across the entity's footprint. We suggest this would help avoid the "monitor all, but 100% is not required" concept in the current language.

Part 6.2: Southern Company suggests this requirement part is unnecessary (it is covered by 6.6), raises many questions, and adds evidence burden with no direct reliability benefit. It is a necessary step in the monitoring *process*, but not a security objective for a standard. We suggest stating the expected result of INSM rather than step by step procedural "how". Explicitly requiring a "collect the needed data" as a requirement requires not only an evidence burden, but brings with it all the questions of missing data, temporarily malfunctioning equipment, data retention to prove the logging is 100% complete, etc. We suggest deletion of this part.

Overall: Are all security objectives for the internal network inside the ESP also required of the systems outside the ESP in the "CIP Networked Environment?" For example, if the EACMS or PACS in scope are on the corporate network, does CIP-007 R6 require the detection of new devices or connections on the corporate network as well?

Vendor Support: This section of the Technical Rationale and SDT presentations explicitly denies any “per system capability” or allowance for vendor issues where they may not allow for modification of tightly engineered and integrated control systems that are maintained and/or warranted by the vendor. The statements that entities should upgrade due to monitoring requirements, where many control system upgrades at plant locations can begin in the $250,000 range and up, we suggest are overreach into large business/operational decisions that should be made by site management in view of all reliability risks that are being managed. With 6.1 currently stating 100% is not required, it seemed odd to have these “no exceptions based on vendor or system capability” type statements in the TR documentation that further cloud what is a compliant scope.

Examples: Southern Company suggests something that will greatly help the entities understand the INSM requirements is to lay out an example of a 1500MW Combined Cycle generation unit that has medium impact BCS, such as 3 separate multi-layered gas turbine control systems for 3 gas turbines, a different multi-layered turbine control system for a heat recovery steam turbine/generator, and a multi-layered DCS for Balance of Plant (BOP) operations – each of these a multi-layer Perdue model system all on one generating unit. Another example that would help is a large, 1500MW+ offshore wind farm with 200+ individual wind turbines. Thinking through examples such as these and what would be a compliant INSM implementation will help the SDT with scoping requirement parts such as 6.1 as well as helping the industry and CMEP personnel understand what a compliant INSM implementation is, not just in data centers and substation control houses, but in the large industrial plant scenarios within the BES.

Likes 0	
Dislikes 0	

Response

In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS and PACS within an ESP are still in scope and should be considered during any INSM implementation. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Technical Rationale has been updated so that Responsible Entities can evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement INSM. The network diagram from the Technical Rationale has been removed.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment
The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. SIGE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. In response to industry comments, the Project 2023-03 DT updated the Technical Rationale so that Responsible Entities can evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement INSM.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment
We appreciate the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot. For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Regarding CIP-008, We urge the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point.

Lastly, we thank the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. In response to industry comments, the Project 2023-03 DT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Whereas CIP-012 communications are between ESPs and are not in scope. Language has been updated accordingly within a new proposed CIP-015 standard and newly proposed three requirements. Regarding CIP-008 comment, this was included as a Measure for Requirement R1, Part 1.3. The term "adversary" has been removed.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to IRC SRC's comments.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	
Document Name	
Comment	
We are concerned with the statements the SDT has included in the Technical Rationale regarding Vendor Support where they state on Page 4: "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents."	

The SDT stating that “every control system should have the capability to provide an appropriate level of visibility” and suggesting that entities will need to update them with modern equipment is unreasonable and may present new risks through new attack vector points into previously isolated systems. This is also in direct contradiction to Requirement R6.1 that allows the entity to assess what level of INSM provides “security value”. Without providing a minimum threshold for monitoring or further guidance on what provides “security value”, there is a lot of room for interpretation into what is required for an entity to meeting compliance with Requirement R6. For those entities that are operating in regulated environments, there is also the possibility of negatively impacting rate payers through costs associated with stranded assets. Including communication between EACMS and PACS systems within the scope of the requirement can create additional obstacles where the systems are managed separately on different networks. There is no guidance provided on how to treat INSM devices that could act as a possible bridge between networks, which would impact compliance with CIP-005.	
Likes 0	
Dislikes 0	
Response	
In response to industry comments, the Project 2023-03 SDT has determined that the scope of the standard being developed should only include networks within each ESP. Note that communications between BCA, PCA, EACMS, and PACS within an ESP are still in scope and should be considered during any INSM implementation. Based on comments received to move the requirements to a new standard or a different existing standard, the DT has created a new proposed Reliability Standard, CIP-015-1, rather than continue to propose revisions to CIP-007. As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version. EACMS and PACS outside of the ESP have been excluded from Draft 1 of CIP-015-1. Project 2023-03 DT updated the Technical Rationale so that Responsible Entities can evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement INSM.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No other comments	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to EEI's comments.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through January 17, 2024
Ballot Pools Forming through January 2, 2024

Now Available

A 35-day formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Wednesday, January 17, 2024** for the following standard and implementation plan:

- CIP-007-X – Cyber Security – Systems Security Management
- Implementation Plan

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.

Reminder Regarding Corporate RBB Memberships
Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools
Ballot pools are being formed through **8 p.m. Eastern, Tuesday, January 2, 2024.** Registered Ballot Body members can join the ballot pools 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

Initial ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **January 8-17, 2024**.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Reminder
Standards Announcement
Project 2023-03 Internal Network Security Monitoring (INSM)

Initial Ballots and Non-binding Poll Open through January 17, 2024

Now Available

Initial ballots and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels for **Project 2023-03 Internal Network Security** are open through **8 p.m. Eastern, Wednesday, January 17, 2024** for the following standard and implementation plan:

- CIP-007-X – Cyber Security – Systems Security Management
- Implementation Plan

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) 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 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 information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through January 17, 2024
Ballot Pools Forming through January 2, 2024

Now Available

A 35-day formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Wednesday, January 17, 2024** for the following standard and implementation plan:

- CIP-007-X – Cyber Security – Systems Security Management
- Implementation Plan

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.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Tuesday, January 2, 2024.** Registered Ballot Body members can join the ballot pools 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

Initial ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **January 8-17, 2024**.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/311)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-007-X IN 1 ST
Voting Start Date: 1/8/2024 12:01:00 AM
Voting End Date: 1/17/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 210
Total Ballot Pool: 256
Quorum: 82.03
Quorum Established Date: 1/17/2024 4:52:41 PM
Weighted Segment Value: 15.42

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	74	1	4	0.077	48	0.923	1	7	14
Segment: 2	7	0.6	1	0.1	5	0.5	0	0	1
Segment: 3	59	1	6	0.125	42	0.875	0	3	8
Segment: 4	10	0.7	2	0.2	5	0.5	0	1	2
Segment: 5	57	1	6	0.136	38	0.864	1	1	11
Segment: 6	42	1	5	0.156	27	0.844	0	2	8
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	1	0.1	4	0.4	0	0	2
Totals:	256	5.8	25	0.895	169	4.905	2	14	46

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		None	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Colorado Springs Utilities	Corey Walker		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Karrie Schuldt		Abstain	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Alain Mukama		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Nazra Gladu	Jay Sethi	None	N/A
1	MEAG Power	David Weekley		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		Abstain	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Platte River Power Authority	Marissa Archie		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Southern Maryland Electric Cooperative	Roger Perkins		Negative	No Comment Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		None	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith		Negative	Third-Party Comments
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Negative	Third-Party Comments
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
5	AEP	Thomas Foltz		Negative	No Comment Submitted
5	AES - AES Corporation	Ruchi Shah		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		None	N/A
5	Austin Energy	Michael Dillard		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		None	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Calpine Corporation	Whitney Wallace		Negative	Comments Submitted
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG Nuclear LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Negative	Third-Party Comments
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Great River Energy	Brian Meloy		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Invenergy LLC	Colin Chilcoat		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Manitoba Hydro	Kelly Bertholet		Negative	Third-Party Comments
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Negative	Comments Submitted
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		None	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 256 of 256 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/311)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT
Voting Start Date: 1/8/2024 12:01:00 AM
Voting End Date: 1/17/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 213
Total Ballot Pool: 254
Quorum: 83.86
Quorum Established Date: 1/17/2024 4:15:36 PM
Weighted Segment Value: 44.89

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	74	1	20	0.377	33	0.623	0	9	12
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	59	1	16	0.333	32	0.667	0	3	8
Segment: 4	10	0.7	3	0.3	4	0.4	0	1	2
Segment: 5	57	1	18	0.409	26	0.591	0	2	11
Segment: 6	41	1	13	0.394	20	0.606	0	2	6
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	2	0.2	1	0.1	0	2	1
Totals:	254	5.6	77	2.514	117	3.086	0	19	41

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Abstain	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Karrie Schuldt		Abstain	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Alain Mukama		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Nazra Gladu	Jay Sethi	None	N/A
1	MEAG Power	David Weekley		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		None	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith		Negative	Third-Party Comments
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Third-Party Comments
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Negative	Third-Party Comments
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	AES - AES Corporation	Ruchi Shah		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		None	N/A
5	Austin Energy	Michael Dillard		Negative	Third-Party Comments
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		None	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Calpine Corporation	Whitney Wallace		Negative	Comments Submitted
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Abstain	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Great River Energy	Brian Meloy		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Invenergy LLC	Colin Chilcoat		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Manitoba Hydro	Kelly Bertholet		Negative	Third-Party Comments
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		None	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 254 of 254 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/311)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-007-X Non-Binding Poll IN 1 NB
Voting Start Date: 1/8/2024 12:01:00 AM
Voting End Date: 1/17/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 206
Total Ballot Pool: 247
Quorum: 83.4
Quorum Established Date: 1/17/2024 4:40:55 PM
Weighted Segment Value: 11.98

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	72	1	4	0.085	43	0.915	13	12
Segment: 2	7	0.5	1	0.1	4	0.4	1	1
Segment: 3	57	1	3	0.073	38	0.927	8	8
Segment: 4	10	0.7	2	0.2	5	0.5	1	2
Segment: 5	55	1	4	0.105	34	0.895	7	10
Segment: 6	40	1	4	0.154	22	0.846	7	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	2	0.2	1	0.1	2	1
Totals:	247	5.5	20	0.917	147	4.583	39	41

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		None	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Colorado Springs Utilities	Corey Walker		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	Dairyland Power Cooperative	Karrie Schuldt		Abstain	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Alain Mukama		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		None	N/A
1	MEAG Power	David Weekley		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Platte River Power Authority	Marissa Archie		Abstain	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	None	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Virginia Power	Bill Garvey		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Entergy	James Keele		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Negative	Comments Submitted
3	MEAG Power	Roger Brand	Rebika Yitna	Negative	Comments Submitted
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Negative	Comments Submitted
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Negative	Comments Submitted
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	DTE Energy	Patricia Ireland		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		None	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		None	N/A
5	Austin Energy	Michael Dillard		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		None	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier	Carly Miller	Negative	Comments Submitted
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	None	N/A
5	Calpine Corporation	Whitney Wallace		Negative	Comments Submitted
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Decatur Energy Center LLC	Megan Melham		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	LS Power Development, LLC	C. A. Campbell		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Negative	Comments Submitted
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Southern Company - Southern Company Generation	Leslie Burke		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Great River Energy	Brian Meloy		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Negative	Comments Submitted
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		None	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 247 of 247 entries

Project 2023-03 Internal Network Security Monitoring (INSM)

Action

- Inform of the Standards Balloting and Comment System impact resulting from the drafting team (DT) creating a new standard after the initial ballot.
- Approve a waiver of provisions of the Standard Processes Manual (SPM) for Project 2023-03 INSM due to regulatory deadlines, as follows:
  - Additional formal comment and ballot period(s) reduced from 45 days to as few as 10 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period (Sections 4.9, 4.12).

Background

Project 2023-03, Internal Network Security Monitoring (INSM), addresses the directives in *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023). Order No. 887 requires NERC to submit new or modified Reliability Standard(s) that require INSM within a trusted Critical Infrastructure Protection networked environment for all high impact bulk electric system Cyber Systems with and without external routable connectivity (ERC) and medium impact BES Cyber Systems with ERC by July 9, 2024.

INSM was posted for an initial ballot that closed January 17, 2024 (January 2024 initial ballot) with 15.42% approval. At an in-person DT meeting that took place January 30, through February 1, 2024, the DT reviewed comments and in response to the comments voted to create a new CIP standard (CIP-015-1) rather than continuing with the initial approach of modifying CIP-007-X.

The creation of CIP-015-1 is the direct result of the Project 2023-03 DT's response to comments following the initial ballot that proposed revisions to CIP-007-X. In response to the comments, the DT decided that rather than moving forward with the proposed revisions to CIP-007-X, it would be preferable to create a new CIP-015-1 Reliability Standard. The SAR clearly provides the DT with the flexibility to "create new or modified existing CIP Reliability Standards".

The DT's decision to create a new CIP Reliability Standard following the January 2024 initial ballot, will be reflected in NERC's system as an initial ballot, as it is the first ballot for Reliability Standard CIP-015. Although the system will reflect the posting as an initial ballot, this posting is an additional ballot per the process laid out in the SPM. As a result, in the next posting, CIP-015-1 will be posted, consistent with the SC approved waiver timeframe for an additional ballot.

NERC Standard Processes Manual Section 16.0 Waiver provides as follows:

- The Standards Committee may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
  - In response to a national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber attack on the Bulk Electric System
  - Where necessary to meet regulatory deadlines

- Where necessary to meet deadlines imposed by the NERC Board of Trustees
- Where the Standards Committee determines that a modification to a proposed Reliability Standard or its Requirement(s), a modification to a defined term, a modification to an Interpretation, or a modification to a Variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.

At the August 2023 Standards Committee (SC) Meeting, the SC approved a waiver of certain provisions of the SPM for Project 2023-03 due to regulatory deadlines, as follows: (1) additional formal comment and ballot period(s) reduced from 45 days to as few as 20 calendar days, with ballot(s) and non-binding poll(s) conducted during the last five days of the comment period; and (2) final ballots reduced from 10 days to as few as five calendar days.

Due to the Federal Energy Regulatory Commission's July 9, 2024, deadline, and the 15% approval rating for the initial ballot, the SC is being asked to consider a waiver of these provisions for Project 2023-03 to shorten the additional comment period(s) further. This is necessary for the DT to have sufficient opportunity to obtain stakeholder feedback and develop a consensus standard by the July 9, 2024, FERC deadline.

Summary

DT leadership and NERC staff recommend shortening the additional formal comment and ballot period(s) for Project 2023-03 from 45 days to as few as 10 days, with a ballot and non-binding poll concurrent during the last 5 days of the comment period.

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024

Anticipated Actions	Date
20-day formal comment period with ballot	02/27/2024 – 03/18/2024
5-day final ballot	TBD
Board adoption	TBD

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:** Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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. Reliability Coordinator

4.1.5. Transmission Operator

4.1.6. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

4.2.1.2 Each Special Protection System (SPS) where the SPS 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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the CIP-002-identification and categorization processes.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Identify network data collection locations and methods, based on the network security risk(s), to monitor network activity including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.

M1. Evidence must include each of the applicable documented process(es) that collectively include each of the applicable requirement parts in Requirement R1 and additional evidence to demonstrate implementation as described in the measure parts. Examples of evidence may include, but are not limited to, one or more of the following for each Part:

Part 1.1

- Architecture documents or other documents detailing data collection methods; or
- Documented rationale on how network locations were selected or excluded for data collection.

Part 1.2

- Detection events;
- Configuration settings of INSM monitoring systems; or
- Documentation of a baseline used to monitor against unauthorized network activity.

Part 1.3

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of responses to detected anomalies, etc.; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Responsible Entity shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M2. Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of unauthorized deletion or modification.

R3. Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Examples of evidence may include, but are not limited to, documentation of the data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to perform the analysis of actionable anomalous activity.

C. Compliance

1. Compliance Monitoring Process

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement one or more method(s) to detect anomalous activity using the data collected at locations identified in Part 1.1. OR The Responsible Entity did not implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.	The Responsible Entity did not include any of the applicable requirement parts to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3). OR The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1).
R2.	N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (except during CIP Exceptional Circumstances).

R3.	N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances).

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

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~~	~~03/22/2023~~
~~SAR posted for comment~~	~~04/06/2023 – 05/05/2023~~

~~Anticipated Actions~~	~~Date~~
~~35-day formal comment period with ballot~~	~~12/14/2023 – 1/17/2024~~
~~XX-day formal comment period with additional ballot~~	~~TBD~~
~~XX-day final ballot~~	~~TBD~~
~~Board adoption~~	~~TBD~~

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 – System Security Management

2. **Number:** CIP-007-~~X~~

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural 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 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 Special Protection System (SPS) where the SPS 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-007-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-002-5.1 identification and categorization processes.

5. Effective Date: See Implementation Plan for CIP-007-X.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-X Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: PCA; and 1. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R2 – Security Patch Management*. *[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-007-X Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R2 – Security Patch Management			
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	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-X Table R2 – Security Patch Management			
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	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-X Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R3 – Malicious Code Prevention			
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	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	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	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-X Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	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	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-X Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	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	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-XTable R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-X Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – Internal Network Security Monitoring (INSM)* to increase the probability of detecting an attack that has bypassed other security controls. *[Violation Risk Factor: Medium] [Time Horizon: Same-Day Operations and Operations Assessment].*

M6. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-X Table R6 – INSM* and additional evidence to demonstrate implementation as described in the Measures column of the table.

~~CIP-007-X Table R6 – INSM~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~6.1~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~	~~Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.~~	~~Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods.~~

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

~~CIP-007-X Table R6 – INSM~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~6.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~	~~Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.~~	~~Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.~~

~~CIP-007-X Table R6 – INSM~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~6.5~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS that perform access control functions;~~ ~~2. PACS that rely upon EACMS that perform access control functions; and~~ ~~3. PCA.~~	~~One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.~~	~~Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.~~

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary.

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 Enforcement Program

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R1. (R1)
R2.	The Responsible entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	included the applicable items in CIP-007-X Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	or revised within the timeframe specified in the plan. (2.4)
R3.	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R3. (R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)
R4.	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented	The Responsible Entity has documented and implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more	process(es) that included the applicable items in CIP-007-X Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) to identify undetected Cyber Security Incidents by reviewing an entity- determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	
R5.	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts.	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-X Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access, but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar	process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			months of the last password change. (5.6)	obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)
~~R6.~~	~~The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).~~	~~The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).~~	~~The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3).~~ ~~OR~~ ~~The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices,~~	~~The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6).~~ ~~OR~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~and network communications using data from Part 6.2 (6.4).~~ ~~OR~~ ~~The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).~~	~~The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1).~~ ~~OR~~ ~~The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).~~

C. Regional Variances

None.

D. 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	Approved 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-007-5.	
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	2/15/15	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-007-X. Docket No. RM15-14-000	
X	06/2023	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on xx/xx/xx. Revised version addresses Order No. 887 related to Internal Network Security Monitoring.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address the three security issues. In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and

[1] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

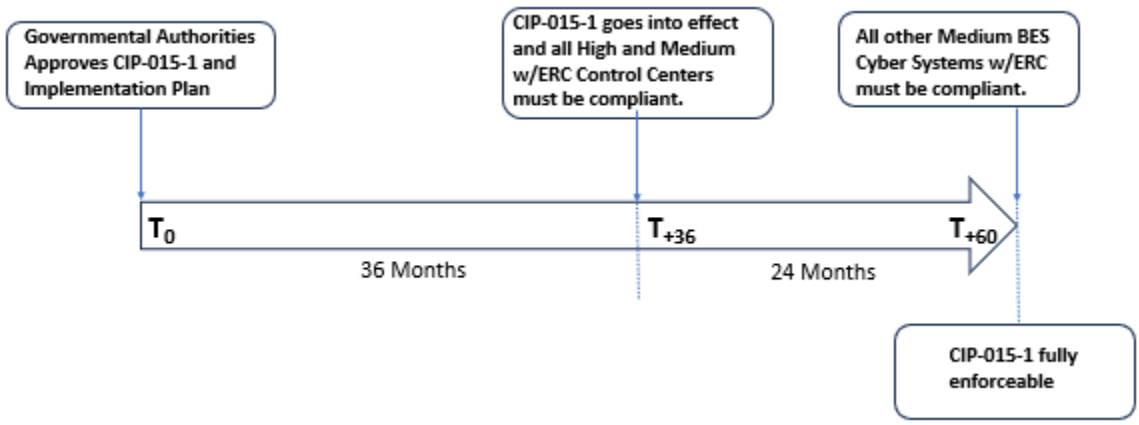
Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided 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 thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1 and R1.2 shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM)
Reliability Standard CIP-~~007~~015-~~X~~1

Applicable Standard(s)

- CIP-~~007~~015-~~X~~ 1 – ~~Cyber Security – System Security Management~~Internal Network Security Monitoring

Requested Retirement(s)

- ~~CIP-007-7 – Cyber Security – System Security Management~~[1]None

Applicable Entities

- Balancing Authority
- Distribution Provider[2]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address the three security issues. In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

[1] ~~If CIP-007-7 is not in effect, the currently effective version would be retired.~~

[2] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC ~~is currently conducting the~~has completed this study~~,~~ and it was ~~which is to be~~ filed with FERC ~~by~~ on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement ~~new~~ Requirements R1, R2, and R3~~6~~. In order to achieve the objectives of the ~~Requirement~~ requirements~~R6~~, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with ~~the new requirements specific to~~ Reliability Standard CIP-~~007~~015-~~X~~1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-~~007~~015-~~X~~ 1 ~~Cyber Security – System Security Management~~Internal Network Security Monitoring

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 thirty-six (36) 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.

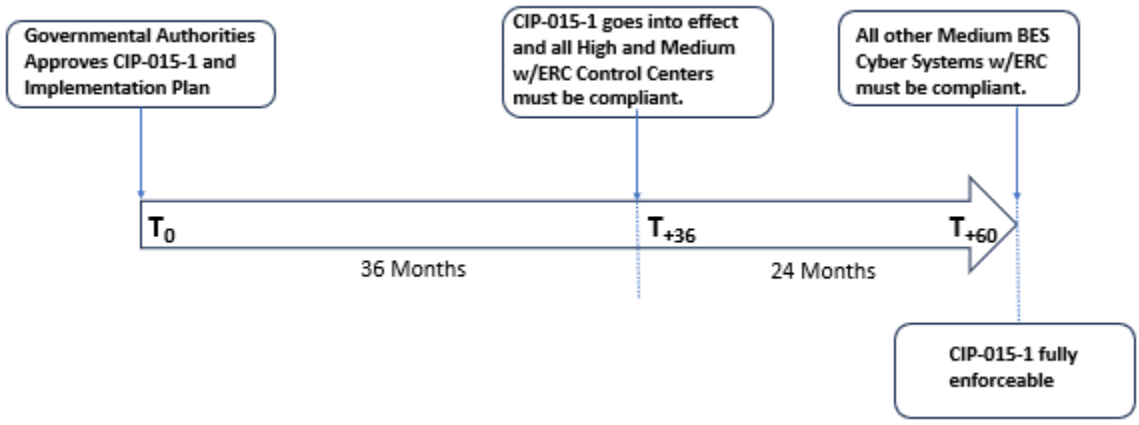
Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-~~007~~015-~~X~~ 1 ~~Cyber Security – System Security Management~~Internal Network Security Monitoring ~~- Requirement R6~~

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1 and R1.2 shall initially comply with the requirements in CIP-~~007~~015-~~X~~ 1 ~~Requirement R6~~ for those Control Centers upon the effective date of Reliability Standard CIP-~~007~~015-~~X~~1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control

Centers. It further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-~~007~~015-~~X~~1 ~~Requirement R6~~ within 24 calendar months after the effective date of Reliability Standard CIP-~~007~~015-~~X~~1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



~~Retirement Date~~

~~**Reliability Standard – CIP-007-7 Cyber Security – System Security Management**~~
~~Reliability Standard CIP-007-7[3] shall be retired immediately prior to the effective date of Reliability Standard CIP-007-X in the particular jurisdiction in which the revised standard is becoming effective.~~

[3] ~~If CIP-007-7 is not in effect, the currently effective version would be retired.~~

Unofficial Comment Form

Project 2023-03 Internal Network Security Monitoring

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2023-03 INSM/CIP-015-1 – Internal Network Security Monitoring** by **8 p.m. Eastern, Monday, March 18, 2024.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Laura Anderson, or at 404-782-1870.

Background Information

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for Internal Network Security Monitoring (INSM) of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard requirements for any new or modified CIP Reliability Standards that address three security issues.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

The Project 2023-03 Drafting Team (DT) Draft 1 of proposed CIP-015-1 requires responsible entities to implement a Network Security Monitoring (NSM) system. Responsible Entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks.

INSM refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the trusted CIP related operational zones of the responsible entity.

Order No. 887 included the phrase "CIP-Networked Environment," which was not specifically defined in Order No. 887, INSM. In the initial posting, the DT included in its proposed revisions communications

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 provides that any new or modified CIP Reliability Standards should address (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; ad (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *See id.* P 5.

between EACMS (e.g., Active Directory, 2FA, or RADIUS) and PACS outside of the ESP as part of the CIP-Networked Environment. Order No. 887 specifically excluded some components of a "CIP-Networked environment;" including low impact BES Cyber Systems (BCS) and medium impact BCS without ERC.

Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. The DT made this decision based upon: (1) industry overwhelmingly agreeing that the order was not broad enough to include EACMS and PACS outside of the ESP within the scope of Project 2023-03; and (2) the inclusion of EACMS and PACS introduced a number of difficult technical complications, e.g., the need to define CIP-Networked environment and how to facilitate the technical inclusion of EACMS and PACS.

In the initial posting, the DT initially proposed revisions to CIP-007. However, in response to comments on the initial posting, the DT has decided to no longer propose any revisions to CIP-007 and, instead, to create a new Reliability Standard, CIP-015-1, Internal Network Security Monitoring. To inform this decision, the DT primarily considered Order No. 887, schedule expectations, and the fundamental principles of INSM. The DT voted unanimously to create a new CIP-015 standard rather than continue with revisions to CIP-007.

Questions

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity's ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the requirement part. Do you agree that the proposed CIP-015-1 Requirement R1,

Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

☐ Yes
☐ No

Comments:

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

    ☐ Yes
    ☐ No

    Comments:

11. Please provide any additional comments for the DT to consider, if desired.

    Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) for INSM high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESP to increase the probability of detecting anomalous or unauthorized network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es), the VRF is reflective of the implementation as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement one or more method(s) to detect anomalous activity using the data collected at locations identified in Part 1.1. OR The Responsible Entity did not implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.	The Responsible Entity did not include any of the applicable requirement parts to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3). OR The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1).

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (except during CIP Exceptional Circumstances).

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 except during CIP Exceptional Circumstances. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances).

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

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 2023-03 INSM. 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-007, Requirement R1**~~

~~The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VSL Justification for CIP-007, Requirement R1**~~

~~The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VRF Justification for CIP-007, Requirement R2**~~

~~The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VSL Justification for CIP-007, Requirement R2**~~

~~The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VRF Justification for CIP-007, Requirement R3**~~

~~The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VSL Justification for CIP-007, Requirement R3**~~

~~The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VRF Justification for CIP-007, Requirement R4**~~

~~The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VSL Justification for CIP-007, Requirement R4**~~

~~The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VRF Justification for CIP-007, Requirement R5**~~

~~The VRF did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

~~**VSL Justification for CIP-007, Requirement R5**~~

~~The VSL did not change from the previously FERC-approved CIP-007-6 Reliability Standard~~

VRF Justifications for CIP-~~007~~015-~~X~~1, Requirement ~~R6~~R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) for INSM high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESP to increase the probability of detecting anomalous or unauthorized network activity. ~~an attack that has bypassed other security controls.~~ The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es), the VRF is reflective of the implementation as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement ~~R6~~ R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium for Requirement ~~R6~~ R1 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VRF Justifications for CIP-~~007~~015-~~X~~1, Requirement ~~R6~~R1	
Proposed VRF	**[High, Medium, Lower]**
than One Obligation	

VSLs for CIP-~~007~~15-~~X~~1, Requirement ~~R6~~R1			
Lower	**Moderate**	**High**	**Severe**
~~The Responsible Entity did not implement one or more method(s) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Part 1.3.~~ ~~The Responsible Entity did not develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity (6.6).~~ N/A	~~The Responsible Entity did not develop one or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary (6.7).~~ N/A	The Responsible Entity did not implement one or more method(s) to detect anomalous activity using the data collected at locations identified in Part 1.1. OR The Responsible Entity did not implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.~~The Responsible Entity did not evaluate the collected data to document the expected network communication baseline (6.3).~~ ~~OR~~ ~~The Responsible Entity did not deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2 (6.4).~~ ~~OR~~ ~~The Responsible Entity did not deploy one or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action (6.5).~~	The Responsible Entity did not include any of the applicable requirement parts to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3). OR The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1). ~~The Responsible Entity did not include any of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls (6.1-6.6).~~ ~~OR~~ ~~The Responsible Entity did not identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to~~

			~~monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks (6.1).~~ ~~OR~~ ~~The Responsible Entity did not log collected data regarding network communications at the network locations identified in Part 6.1 (6.2).~~

VSL Justifications for CIP-~~007~~015-~~X~~1, Requirement ~~R6~~R1~~1~~	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	Moderate	High	Severe
N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (except during CIP Exceptional Circumstances).

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	[High, Medium, Lower]
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. ~~Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.~~.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 except during CIP Exceptional Circumstances. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	Moderate	High	Severe
N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances).~~N/A~~

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, but only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats and incidents. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the operational zones of the entity. While the entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following security issues: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices within the ESP of applicable BES Cyber Systems.

The Project 2023-03 DT proposed Reliability Standard CIP-015-1 requires responsible entities to implement INSM processes. Responsible Entities must evaluate their networks within ESPs and identify the collection location(s) and method(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. That could include escalation to an entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition.

Responsible Entities must also appropriately protect the collected INSM related network communications data and metadata to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. In addition, entities must retain relevant data collected from their INSM system(s) with sufficient detail and duration to facilitate the evaluation and further investigation of potential cybersecurity incidents. INSM will be an on-going, or possibly an iterative, process enabling responsible entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The Drafting Team considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887[3], schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Based on industry comments, the DT concluded that INSM requirements do not fit cleanly into any existing standard and would be best implemented as a standalone standard. In addition, developing a new standard provides future standard development teams with a framework for potential expansion of INSM to mediums without ERC and low impact BES Cyber Systems, if needed.

[3] *Id.*
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

System Classification

The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[6]" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM

The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While an entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not expected or required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Summary

Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within protected ESP environments.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Identify network data collection locations and methods, based on the network security risk(s), to monitor network activity including connections, devices, and network communications*."*

As described in Richard Bejtlich's book, The Practice of Network Security Monitoring, monitoring is most effective when collection occurs at strategic network locations and utilizes a variety of methods. In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1 requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.

[6] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1 requires that Responsible Entities evaluate their internal ESP networks and select an INSM data collection location(s) and method(s) that provide the necessary data to implement Requirement R1, Parts 1.2 and 1.3. Requirement R1, Part 1.1 allows Responsible Entities latitude to select data that provides value based on a Responsible Entity's evaluation of the network cybersecurity risk in their particular system.

Data Collection Locations

In CIP-015-1, "network data collection locations" refers to both a physical and a logical concept. In a physical context, network data collection locations connote data collection from devices that perform technical functions within and between networks, such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. An entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cybersecurity monitoring value from the collection system. In another example, an entity may identify physical traffic to and from a specific operational host such as a Human Machine Interface (HMI) and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

The entity is responsible for identifying physical and logical communication convergence points that will provide the highest value data for the INSM system.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Usually not ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although responsible entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected.

	Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an extensible authentication protocol (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Capable of performing in low bandwidth environments. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments. High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Optional considerations for selecting or excluding collection locations and methods

As Responsible Entities determine collection locations and methods, the following considerations might inform the decision for including or excluding a collection location or method:

Adversary Analysis

The entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive collection priorities to focus on targeted threats and uses cases that would inform collection locations and exclusions.

ICS Protocols
INSM technologies are most meaningful and effective when they are built to be ICS protocol aware and provide detections of network activity that might hamper an industrial process. The collection locations and methods, as well as the analysis tools used for INSM, should be assessed for their capability to detect ICS specific attacks.

Data Types
The Mitre ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation
2. Network Traffic Content
3. Network Traffic Flow

While selecting data locations and methods, an entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication
Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network collection locations and methods. Consideration of traffic duplication may be part of a rationale on how network locations were selected or excluded for data collection.

Complimentary Monitoring Systems
Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data collection locations.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network locations were selected or excluded for data collection.

A Responsible Entity with mature firewall logging capabilities and extensive segmentation may choose to include firewall logs to augment INSM collection.

Aligning Collection and Monitoring with Operations
Operational changes might require temporary or extended removal of INSM collection at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R1, Part 1.2 or 1.3. For

example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alarms in some INSM systems. Suppressing alarms or collections may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic;
2. High rates of false positive alerts until tuning can be completed;
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility should not justify a potential non-compliance finding, especially when other cybersecurity monitoring is in place.

External Networks

External networks, such as turbine monitoring systems, Inter-Control Center Communications protocol (ICCP) connections, etc., are high value networks for INSM data collection of data related to these functions is more likely to be selected than excluded from network data collection.

Resilience

While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1 allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN

Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering

Filtering or elimination of traffic with low cybersecurity value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection

Requirement R1, Part 1.1 does not require collection of data such as:

- Serial communications
- 4-20ma circuits
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used)

Vendor Constraints

Some ICS vendors have historically stated that their systems do not support cybersecurity monitoring using either INSM data collection or endpoint logging collection. Rather than add a "per system capability" exclusion, Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and data collection methods appropriate to each entity's ESP networks.

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Entities are not expected to implement all of these, but rather to choose and implement the collection locations and methods that provide the most value to the entity.

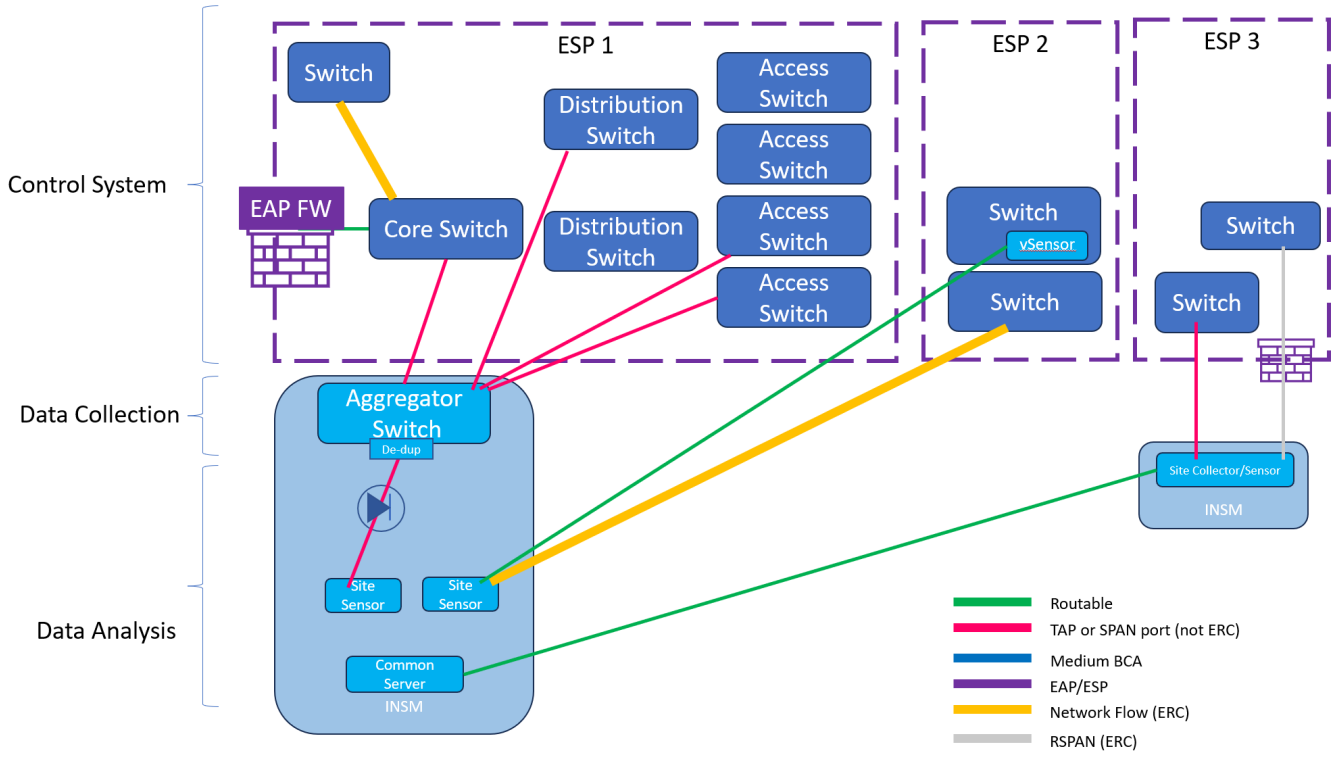


Figure 1

This reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of the rise of AI on the technology landscape, new anomalous detection products that use AI learning models are likely to be introduced. It is not the intent of the DT to dictate what technology an entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement 1, Parts 1.2 and 1.3.

Rationale for Requirement R1, Part 1.2

> *Requirement R1, Part 1.2:* "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2 will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and the INSM Requirement R1 and Requirement R1, Part R1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

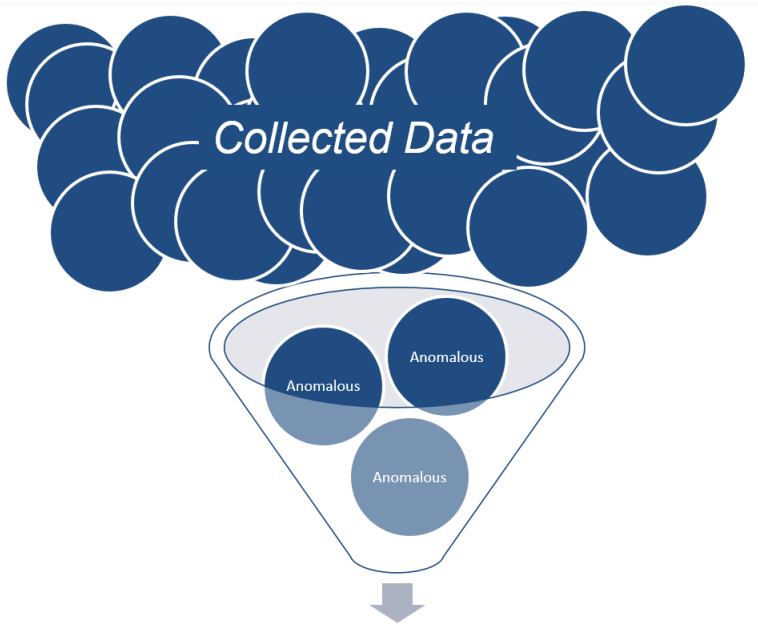


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Anomaly detection is sometimes referred to using other names such as modeling. Products may include machine learning algorithms and other technology to reduce the number of notifications.

Signature-based detections

Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.

When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2, attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for metadata retention in Requirement 2.

Behavioral Detections

Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning

After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking

INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods

Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning

Cybersecurity detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3

*Requirement R1, Part 1.3: "*Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action."

Evaluation of activity detected in Requirement R1, Part 1.2 is the "analyze" step described in Bejtlich's book. Analyzing the data is an expected part of cybersecurity operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions an entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Registered Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

Rationale for Requirement R2

*Requirement R2: "*Responsible Entity shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.''

A common adversary technique is "Indicator Removal" (T1070[7]). The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls like those used to protect BCSI or EACMS. Examples of controls that should be considered to safeguard INSM data include:

- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Granting only authorized personnel access to the INSM system.
- Segmentation of the INSM system into an isolated network separate from operational technology (OT) and corporate networks.

[7] https://attack.mitre.org/techniques/T1070/

- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Note that no part of Reliability Standard CIP-015-1 or Requirement R2 is intended to limit information sharing. The focus of Requirement R2 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cybersecurity program. Government agencies expect and encourage registered entities to share information gathered by INSM systems (see NIST 800-150[8], CISA Information Sharing Guidance[9], Cybersecurity Information Sharing act of 2015[10]).

The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[11]" states that the CIP-011 Requirement R1, Part 1.2 process "should include how the registered entity addresses providing BCSI to third party vendors or other recipients." After implementing INSM entities may need to review their CIP-011 Requirement R1, Part 1.2 process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

Rationale for Requirement R3

> *Requirement R3: "*Responsible Entity shall implement one or more documented process(es) to retain network communications data and other metadata collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.''

Requirement R3 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3 and provide evidence needed to meet CIP-008-6 Requirement R3 for data retention related to an actual cybersecurity incident or attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

[8] https://csrc.nist.gov/pubs/sp/800/150/final
[9] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[10] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[11] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Network Communications Data Type	Cybersecurity Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Registered Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Registered Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Registered Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system. Specifying retention timeframes as averages or moving targets rather than absolute values is an acceptable specification in a data retention chart.

Metadata

In the context of Requirement R3, INSM related metadata is a record of past network communication and traffic or a summarization of that traffic.

Metadata retention will vary by protocol. For example, some ICS protocols do not use layer 3, and other ICS protocols are layer 3, but do not create TCP connections. The decision and capabilities of what metadata is retained is frequently configured as part of the INSM system. Registered Entities should consult with vendors to ensure that INSM tools store sufficient data to support necessary analysis of

network activity. The decision of which metadata to store and retention timeframes should enable the entity to accomplish its cybersecurity and operational objectives.

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through March 18, 2024

Now Available

A 20-day formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Monday, March 18, 2024** for the following standard and implementation plan:

- CIP-015-1 – Internal Network Security Monitoring
- Implementation Plan

Following the January 2024 initial ballot and comments received, the DT decided to create a new CIP Reliability Standard. The new CIP Reliability Standard will be reflected in NERC's system as an initial ballot, as it is the first ballot for Reliability Standard CIP-015. Although NERC's system will reflect the posting as an *initial ballot*, this posting is an ***additional ballot*** for Project 2023-03. The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.

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.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools

The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.

- *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

Initial ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 12-18, 2024**.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | Draft 1 of CIP-015-1
Comment Period Start Date:	2/27/2024
Comment Period End Date:	3/18/2024
Associated Ballots:	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 IN 1 ST Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 73 sets of responses, including comments from approximately 160 different people from approximately 102 companies representing 7 of the Industry Segments as shown in the table on the following pages.

Questions

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity's ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

5, Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

11. Please provide any additional comments for the DT 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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO

					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	1	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
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
					John Nierenberg	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
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Jason Procuniar	Buckeye Power, Inc.	4	RF
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE
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

					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
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
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Dominion - Dominion	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion	3	NA - Not Applicable

Resources, Inc.						Resources, Inc.		
					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
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
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
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

Gary Dollins	M and A Electric Power Cooperative	3	SERC
William Price	M and A Electric Power Cooperative	1	SERC
Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC
Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
Tony Gott	KAMO Electric Cooperative	3	SERC
Micah Breedlove	KAMO Electric Cooperative	1	SERC
Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
Jarrod Murdaugh	Sho-Me Power Electric Cooperative	3	SERC

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy supports this change, and thanks the Drafting Team for their careful consideration of the scope.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 supports the modifications.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.

Likes 0	

Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
A PCA is within an ESP, the question is worded incorrectly.	
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 comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
The term “PCA devices outside of the ESP” appears to contradict the NERC definition of PCA.	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF supports this change, as the previous conditional inclusions were a source of confusion for many.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA endorses removing "EACMS, PACS, and PCA devices" from the requirements.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Southern Company appreciates the change in scope for this version of the standard. The original scoping in the standard for individual systems outside of a defined ESP in requirements intended at a network (and not system) level is problematic. If the intent of the standard included system level monitoring rather than network monitoring only, how to scope such requirements to individual systems would be clearer. We appreciate the clearer scope.	
Likes 0	
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments for all questions	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments for all questions.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	

Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST recommends that, for the sake of consistency with CIP-007, CIP-015's scope include BES Cyber Assets and any associated PCAs (which exist only inside ESPs).	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
WECC agrees with not including EACMS, PACS and PCAs outside ESP as it would not be consistent with the applicable systems scope of the SAR. However, we note that any scope of 'PCA devices outside of the ESP' is not supported by the definition of a PCA – 'One or more Cyber Assets connected using a routable protocol **within or on an Electronic Security Perimeter** that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.'	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	

Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	
A PCA is within an ESP and the question is worded incorrectly	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
EEI agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Don’t see the issue, but the final requirement verbiage should be clear on the Applicable System(s)/ESP.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon is aligning with the EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	Yes
Document Name	

Comment

ITC supports EEI's comments on this project.

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:

"A PCA is within an ESP and the question is worded incorrectly. "	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
PCA devices do not sit outside of the ESP. Please clarify if the DT intention is to exclude PCA devices (in the ESP) or to simply exclude EACMS and PACS (outside of the ESP).	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 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	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
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	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
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	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
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	

Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	
Document Name	
Comment	
SUPPORTING EEI COMMENTS ON ALL QUESTIONS.	
Likes 0	
Dislikes 0	
Response	

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

SRP could support the creation of an entirely new standard once we understand the definition of “objective-based”. Please clarify “objective-based” or explain what it actually means.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

If INSM not going to be in CIP-007 R6 and creating CIP-015 for INSM, why not move CIP-007 R4 Security Event Monitoring also to this new CIP-015?

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.

Likes 0	

Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	

Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	

Response
Daniel Gacek - Exelon - 1
Answer	Yes
Document Name	
Comment
Exelon supports the comments submitted by the EEI for this question.
Likes 0	
Dislikes 0	
Response
Kinte Whitehead - Exelon - 3
Answer	Yes
Document Name	
Comment
Exelon is aliging with the EEI in response to this question.
Likes 0	
Dislikes 0	
Response
Robert Blackney - Edison International - Southern California Edison Company - 1
Answer	Yes
Document Name	
Comment
See comments submitted by the Edison Electric Institute.
Likes 0	
Dislikes 0	
Response

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards	
Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3

Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
While TVA understands the challenges to updating CIP-007 to include internal network security monitoring we believe that these changes should be included within existing monitoring requirements or those requirements, mainly CIP-007 R4, be moved to CIP-015 as well. INSM should be an extension of the existing required cybersecurity monitoring program, not a new program. By combining the two efforts some of the same requirements between CIP-007 R4 and the INSM components in CIP-015 may be used. Additionally, if the scope of the standard is expanded to Low systems in the future this will make it easier to apply the full monitoring program that would be needed. Moving the proposed monitoring requirements to CIP-015 removes these obligations from the scope of the existing CIP-003 Cyber Security Policy – suggest consider revising CIP-003 to include CIP-015 in Cyber Security Policy.	
Likes 0	
Dislikes 0	

Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 supports the modifications.	
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	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Wilke - American Transmission Company, LLC - 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	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
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	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
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	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 2	

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports this change and agrees that a new standard is the best approach to incorporating the INSM revisions.	
Likes 0	
Dislikes 0	
Response	

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity's ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer	No
Document Name	

Comment

AES supports EEI comment below

EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

Tri-State agrees with EEI comments below:

"EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."

Likes 0	
Dislikes 0	

Response

Wendy Kalidass - U.S. Bureau of Reclamation - 5

Answer	No

Document Name	
Comment	
Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous (*remove:* or unauthorized) network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. Suggest R1 be rewritten to state that the standard requires monitoring of the network within an ESP to include all systems that are connected therein, whether permanent or temporarily (such as Transient Cyber Asset).	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

FirstEnergy believes clear separation of where CIP-005 ends and where CIP-015-1 begins in terms of enforcement would benefit the scope of CIP-015-1.

Since 'internal network security monitoring' will not be a defined term and Technical Rationale explanation are not part of the enforceable Requirement, FE asks the Drafting Team to more clearly identify their technical rationale in the standard so as to "help" Responsible Entities define that term for themselves, understanding the baseline knowledge of NERC and its Regional Entities.

Finally, FirstEnergy suggest removal of the conjunctive “or unauthorized” in the opening sentence of R1. The use of the term “unauthorized” hints at this should include some sort of authorization process paperchase for every network communication which is impractical and not related to potentially malicious network traffic.

Likes 0	
Dislikes 0	

Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company agrees with the feedback by EEI. In addition, Southern has concerns with the phrase “increase the probability of detection” as the stated objective. Southern agrees that such a concept is necessary to prevent R1 from requiring 100% perfection of detection which no tool can guarantee. As this phrase is the core of the requirement's objective and what it is to accomplish, the focus is on an "increase" in probability and thus how your process accomplishes this increase, rather than whether the entity has implemented a process that can meet 1.1 to 1.3. A suggestion is to replace the phrase with “provide the capability of detection” or similar phrasing that is a far more binary judgment to make (did the entity implement a process to provide detection capability to meet all the requirement parts) and still avoids the 100% perfect detection of every anomaly issue. Therefore, if minimal change to R1 is required, we suggest the following (though we have a further suggestion of a more substantive change for consideration in Q4):

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability **provide the capability** of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

Likes 0	
Dislikes 0	

Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE support's EEI's comment(s): EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD agrees with the comments submitted by Tacoma Power, and that the suggested language change to R1 is non-substantive and could be made for the final ballot posting.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy supports EEI comments

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment
Project 2016-02 modified the concept of an EPS to include Zero-Trust architectures, where there is no “inside” or “outside” an ESP, but rather relies on the idea of “protected by an ESP.” Tacoma Power Suggests the following language for CIP-015 R1: “Implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) or a medium impact BCS with External Routable Connectivity (ERC), **protected by an ESP**, to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]” Tacoma Power thinks the language change to R1 is non-substantive and could be made for the final ballot posting.

Likes 0	
Dislikes 0	

Response

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment
Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	

Comment
BHE appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	

Comment	
Clarity is required if INMS requirement is also applied to EACMS/PACS/PCA within ESP.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	

ITC supports EEI’s comments on this project.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments:

"The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. NPCC RSC proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP."

Likes 0	
Dislikes 0	

Response

Hillary Creurer - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Minnesota Power supports EEI’s comments.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

SRP feels that there are no methods to measure compliance as the standard is stated. We ask to provide guidance as to what is required as evidence. Should detection be continuous, or is periodic detection permissible? Also, there is no timeline as to how often detection and evaluation should be performed (In real time? Every 15 minutes? Every 15 months?).

The standard does not make it clear of the word "baseline" is. Perhaps, the "defintion" or the expectation of what the baseline is should be in the measures section. The technical rationale "definition" of a baseline is more clearly defined under Detection Methods "Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.". However, we did not see any reference to what is in the methods for this wording.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

There is not a definition of "Network" in network security monitoring. While our *understanding* is that this standard is focused on network traffic monitoring, it is not explicit and, therefore, could be interpreted in multiple ways (EDR vs East/West traffic monitoring vs full network traffic monitoring, for example).

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

"Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of ***detecting anomalous network activity***. The documented process(es) shall include each of the applicable requirement parts."

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	
Seminole Agrees with the comments provided by EEI "EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."	
Likes 0	
Dislikes 0	
Response	

Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the parent requirement R1 of CIP-015-1 clearly addresses INSM within a Responsible Entity's ESP.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent and supports 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 supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF supports this clear direction.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Existing monitoring standards are prescriptive to specific locations and event types that are possible to be monitored through traditional log review and automated evaluation. R1 is vague in the specific requirements that must be included in a process. Anomalous network activity is not defined within the standard or the glossary. This is left up to interpretation of the entity and the auditors. In the measures “Architecture documents” is beyond what is required for Electronic Security Perimeter drawings in CIP-005. Request for drawings should be limited to inclusions of elements within required drawings in the standards. The current draft of the standard also only allows for internal IDS types of solutions with detection event capturing and review.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes

Document Name	
Comment	
PNMR agrees with intent of R1 but suggests changing the language from “to increase the probability of detecting” to “… to detect anomalous or unauthorized network activity”.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
James Keele - Entergy - 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	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
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	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Krabe - Lower Colorado River Authority - 5	
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	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the drafting team's efforts to be responsive to FERC Order No. 887. Texas RE is concerned, however, that the language in Requirement R1 does not lend to consistent application and would be a challenge to audit and enforce. Since the language in Requirement Part 1.1 does not establish a minimal level of acceptable monitoring or establish a maximum level of risk acceptance, an entity could determine that there are no network data collection locations and methods. If there are no network data collection locations and methods identified, Requirement Parts 1.2 and 1.3 would not be relevant. Texas RE recommends clarifying "network security risk(s)". The SDT could consider including network security risk criteria similar to how CIP-002 includes impact rating criteria or establishing minimum security risks similar to how CIP-007 Requirement R4 requires logging a minimum of certain types of events.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. TFIST proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP	
Likes 0	

Dislikes 0	
Response	

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6

Answer	No
Document Name	

Comment

Seminole agrees with comments from EEI

“EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: “Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications.” EEI proposes modifications to the draft M1, Part 1.1 measures to: “Architecture documents or other documents detailing data collection location(s) and method(s); or”

Seminole also agrees with Comments from Entergy

“ The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider all possible network data collection locations. For example, and entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.”

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

BHE appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	
Response	

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

"Identify network data collection **point(s)** based on the network security **threat(s) and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	
Comment	
M1 1.1 - The term "documented rationale" is very open and can be a place where professional opinions may differ. A registered entity may have one an effectve approach to monitoring but an auditor may have a differing opinion. While flexibility has it's pro's and con's, some entities may prefer to have a little more specificity of what's needed to guide both the entity and regional entity audit staff.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
No objectives to measure compliance have been provided. Self proclaimed compliance would not be auditable (based on RE perception, rather than auditors). It is very vague, there is no measurement to consider what is acceptable. The entity can say I am always in compliance. There is no clear definition on how and how long to save off the data. Also, how to obtain the level of monitoring in the requirement is vague. This will be subjective vs objective. In addition, R1 1.1 states to identify location "based on the network security risk(s)" but does not attempt to quantify specific risk or suggest which level of risk they're seeking to address. While entities can determine their own level of acceptable risk, this could lead to a wide range of outcomes.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	

Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. NPCC RSC suggest removing “Network Security Risk” or stating that INSM should be for monitored of the entire network per technical capability or assess “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly."	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language: “Identify network data collection location(s) **point(s)** and method(s), based on the network security **threat(s)** risk(s) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications.”	

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the drafting team efforts and the opportunity to comment.

The use of the 'risk-based' language in CIP-015 R1.1 is leaving it to the discretion of entities to determine which component poses higher or lower risks. This will leave it open to the auditor's interpretation and expectation instead of ensuring the scope is concise and clear under this requirement. BC Hydro recommends to define the parameters of these 'risks' to give clear direction to entities or specify the network components on which this requirement R1.1 applies.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

BHE requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

"Identify network data collection location(s) **point(s)** and method(s), based on the network security risk(s) **identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with 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 EEI comments	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that instructing Entities to use a "risk-based approach" to designing and implementing INSM could result in endless arguments among Responsible Entities, Regions, and NERC over what might be	

considered acceptable risk-based approaches. We are even more concerned about the proposed criteria for Severe VSL for R1 ("The Responsible Entity did not identify network data collection locations and methods that provide value,..."). What is "provide value" intended to mean, and who would have the final say on whether a given Entity's INSM implementation was capable of doing so?

NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection locations and methods used to monitor network activity including connections, devices, and network communications."

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that the Standard does not address scenarios in which no technical solution is available to achieve what the Standard requires, such as when an entity's environment includes devices that use non-standard communication protocols. The SRC recommends that the standard be revised to address these types of scenarios, such as by allowing entities to apply for a Technical Feasibility Exception if circumstances warrant.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment

NEE is not in agreement with EEI's comment

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	

Comment

AZPS agrees with EEI proposed revision to CIP-015-1 R1, Part 1.1:

"Identify network data collection location(s) **point(s)** and method(s), based on the network security **threat(s)** risk(s) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern agrees with and greatly appreciates the discussion in the TR on Part 1.1 and the degree of flexibility described there to “narrow the focus to collect the data that provides the highest benefit” and “narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data”. However, Southern suggests that R1 as worded implies a scope of 100% coverage of every subnet within in-scope ESPs. It is not until an example under the R1.1 measures that it mentions the potential exclusion of any network locations and the documentation of such.

The TR states many different aspects to consider in choosing monitoring locations (value, benefit, cost-effectiveness, relevance, etc.) but R1.1 limits it to only network security risks. There is concern with the implication of “do all, but explain where you don’t” that this could require the documentation of network security risks for each IP subnet and “prove the negative” type evidence. As page 4 of the TR states network data collection location refers to both physical and logical networks, so there is concern with the large proliferation of logical networks with containerization (what used to be API calls are being replaced with virtual networks and IP addresses assigned to containers). Zero Trust principles and containerization call for ever more micro-segmentation and creation of virtual networks down to this level between components of an application in a single system. As an example, documented reasons of why an entity did not monitor every internal virtual network generated by Docker between two components of a single application within a single Cyber Asset one could argue are of little value, but it seems would be necessary.

For all these reasons, we suggest a concept of a positive “identify where you do” rather than a sense of “explaining and documenting where you don’t”. The value of where to monitor is going to be based on the system’s architecture, especially in large, multi-layered, distributed systems. On the other end of the spectrum is a site that may have a router with an ACL on an ethernet port to an RTU, which is then connected serially to several relays. Monitoring that 2 node, single ethernet cable “internal network” ESP may be of no value as all traffic can be monitored on the other end of the circuit, and it is unclear whether the entity is compliant if they do so.

Southern suggests a concept for R1 and 1.1 such as:

R1. Responsible Entity shall implement one or more documented process(es) for Internal Network Security Monitoring (INSM) that includes:

R1.1 Identification of network data collection points by the Responsible Entity for its high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC).

We suggest that this covers monitoring the in-scope systems, but leaves flexibility on where such monitoring occurs on its networks and doesn’t imply “prove the negative” for every physical/virtual subnet that is not tapped and monitored.

Likes 0	
Dislikes 0	

Response

Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	

Comment

Avista agrees with comments by EEI (words in italics are requested to be struck)

EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

"Identify network data collection *location(s)* **point(s)** and *method(s)*, based on the network security **threat(s)** *risk(s)* **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	No
Document Name	

Comment

"***R1.1*** *Identify network data collection locations and methods,* ***based on the network security risk(s)****, to monitor network activity including connections, devices, and network communications*."

The bolded part ("based on the network security risk(s)") is not clear and can be open to interpretation of what is required. Therefore, it is recommended to require identification of the specific data collection locations and methods based on an entity's own experience and system needs.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The "risk-based" language leaves it open for auditor interpretation. Meaning, auditors can determine that an entity did not apply the appropriate "risk-based" approach for their network security. BPA believes some level of deference must be offered to an entity's risk management approach. Or, create auditor guidance on what a risk-based approach looks like with regards to INSM.

BPA reiterates its comments from the previous comment period regarding 'risk-based approach':

"BPA recognizes and appreciates the SDT's effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors... BPA

suggests that R1.1 be rewritten to more clearly specify the requirement, such as “Use a risk-based assessment methodology to identify network data collection locations and methods…” Language used elsewhere in the CIP Standards, such as “as determined by the Registered Entity”, could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc."

BPA also asks the DT to clarify the term “locations” in the requirement, adding context currently only found in the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. Cogentrix suggests removing “Network Security Risk” or stating that INSM should be for monitoring of the entire network per technical capability or assess “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated clearly in the standard. Furthermore, greater specificity should be offered for what ‘network activity’ entails. For connections, monitored activity should include who, when, why, and how long; network communications should include type, port, bi-direction or unilateral, etc.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider ***all*** possible network data collection locations. For example, and entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI’s comments: EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

“Identify network data collection (*remove*: location(s)) **point(s)** (*remove*: and method(s)), based on the network security **threat(s)** (*remove*: risk(s)) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications.”

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity’s implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0	
Dislikes 0	

Response

Wendy Kalidass - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.

Likes 0	
Dislikes 0	

Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy recommends the use of the word “points” instead of “locations” in R1.1.	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES Support EEI comment below EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: “Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications.” EEI proposes modifications to the draft M1, Part 1.1 measures to: “Architecture documents or other documents detailing data collection location(s) and method(s); or”	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
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 Collaborators	
Answer	Yes
Document Name	
Comment	
While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains “and allow for future expansion if necessary”, makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
While Requirement R1, Part 1.1 is clear in intent, it must be supported by guidance on acceptable methods of monitoring network activity. For example, is monitoring activity at endpoints acceptable, or is dedicated monitoring equipment required? If a zero-trust strategy is implemented, can monitoring attempts to establish connections outside of the zero-trust architecture satisfy this requirement, or is a more traditional network intrusion detection solution required? It may not be practical to address such questions in the standard, but guidance documents that include technology options must reflect and support the intentions of the SDT.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

Georgia System Operations Corporation supports ACES comments: "While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains 'and allow for future expansion if necessary', makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next."

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

SPP respectfully asks the SDT to consider a “per system capability” clause due to potential technology limitations for entities (current and future technologies).

Likes 0	
Dislikes 0	

Response

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer	Yes
Document Name	

Comment

SMECO agrees with ACES comments:

While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains “and allow for future expansion if necessary”, makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	
CIP-015 R1.1 goes beyond the requirements in CIP-007. If we are logging events at a BES system level per the Cyber Asset capability then the network locations are already identified at the layer 2 and layer 3 devices within the scope of the existing cybersecurity monitoring program. By not updating existing monitoring standards the new standards are introducing additional complications to demonstrating how the monitoring program works overall. The statement based on network security risk(s) is vague on what risk should be evaluated or included in the assessment.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
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	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
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

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer	
Document Name	

Comment

The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. TFIST suggest removing “Network Security Risk” or stating that INSM should be for monitored of the entire network per technical capability or assess “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is concerned the enforceable language of the requirement does not specify that the Responsible Entity is required to document the rational/justification for inclusion or exclusion of data collection location(s) and method(s) based on a risk-based approach in determining what data is necessary to monitor network activity. The SDT should consider requiring entities to justify the parameters they have developed to meet the requirement.

The SAR for this project states, “Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communications, and software inside the CIP-networked environment.” Texas RE noticed that software inside the CIP-networked environment is omitted from the requirement language. If the SDT intentionally omitted this language, then no change is needed. If the SDT did not intend to omit the language, Texas RE recommends including software in the requirement language.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3	
Answer	
Document Name	

Comment

The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider ***all*** possible network data collection locations. For example, and entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.

Likes 0	
Dislikes 0	

Response

5, Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	

Comment

AEs Supports EEI comment below

EEI appreciates the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

As described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment

Tri-State agrees with EEI comments below:

"The description of of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

"As described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version. However, It is clear that detection of anomalous activity has to be referenced to some standard/metric so it would appear that a baseline would be required, and as such should be stated explicitly.

Further, this approach appears inconsistent with existing requirements in CIP-007, R4, which calls for generation of alerts for security events. Should not this capability exist for ISNM as well that could then be evaluated in R1.3?

Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST disagrees with the SDT's decision to demote network baselining from a Requirement to a Measure, which is essentially nothing more than a suggestion, for two reasons:

> FERC Order 887 Paragraph 5 states explicitly, "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment."

> We are hard-pressed to imagine how anyone using INSM could detect anomalous network behavior without a baseline. To that point, Order 887 Paragraph 12 states, "Establishing baseline network traffic allows entities to define what is and is not normal and expected network activity and determine whether observed anomalous activity warrants further investigation."

Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No

Document Name	
Comment	
Tacoma Power supports the EEI comments for consistency of language on what to detect (i.e. anomalous or unauthorized). Tacoma Power thinks the language change to Part 1.2 is non-substantive and could be made for the final ballot posting.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version."	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	No
Document Name	
Comment	
Part 1.2 refers to “data collected at locations identified in Part 1.1,” but it seems that depending on the method used to collect and identify anomalous information, the data collection location may not be relevant. Suggested language: “Implement one or more method(s) to detect anomalous network activity using the data collected pursuant to Part 1.1.”	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
This would require knowledge of previous context and in order to be compliant, it appears that a baseline would be required to compare network activity to detect “anomalous” activity. SRP strongly feels that it should be stated specifically in the standard. Also, as previously stated, the requirement is still not clear of the word "baseline" and perhaps a definition or explanation should be included in the measurements section. SRP also suggest that in the Methods it includes what the Technical rational has defined as a "baseline" as the word "baseline" is still confusing since the baseline is also used in CIP-010 R1.	
Likes 0	
Dislikes 0	
Response	
Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	
Seminole supports the comments from EEI “The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees that Part 1.2 is clear and an objective-based approach that requires one of more methods to detect anomalous network activity without the prescriptive requirement of a baseline.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI's comments: EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term "baseline" in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that "[m]any vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not."

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 comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates and endorses this approach, which is clear in its intent. However, there is a concern that the phrase “detecting anomalous or unauthorized network activity” in R1 does not align well with Parts 1.2 and 1.3. We recommend striking “or unauthorized” in R1 to better align with the rest of the standard. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.	
Likes 0	
Dislikes 0	
Response	

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
BPA endorses removing "baseline" language from the requirement.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes

Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the feedback by EEI. In addition, we do note the wording in the 1.2 requirement part is “anomalous”, but the measure switches to “unauthorized”. Per our comment on R1, we would suggest this be changed in the measure to match the requirement. A baseline of normal traffic could be used to show what is anomalous but would not determine what is unauthorized.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Including measures referencing documentation of a network baseline not included in the standard does not make it an obligation of the requirement. Suggest remove from the measures. Instead, suggest the standard list specific events that an entity should be looking for as a minimum requirement.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes

Document Name	
Comment	
PNMR agrees with the SDT to remove the term “baseline” from the requirement language. It does, however, believe that the term “baseline” in the Technical Rationale should be replaced with “expected network behavior”.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support’s EEI’s comment(s): EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”	

Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	

Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
M1 1.2 -The phrase "Documentation of baseline used" does not adequately capture how these tools work. Some entities configure settings of these tools to only alert on exceptions to a baseline, but it's not like the software baseline that is easily discernable. Explicit baselines may be problematic since the tools are typically based on learning to detect anomalies, though feels our approach would be to provide the configuration settings used for the monitoring tool. This is more of a conpliance concern as some entities may leverage other options to demonstrate compliance than a baseline.	
Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

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	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
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	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	

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	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
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 Collaborators	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned with the removal of explicit requirements such as baselining to accomplish the security objective of implementing methods to detect anomalous network traffic. FERC Order No. 887 recognizes that establishing baselines is the primary means to identify anomalous traffic within an entities' CIP-network environment, noting that "any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment." FERC Order No. 887, at ¶ 79. Texas RE notes that FERC Order No. 887 does contemplate that the final rule should "provide flexibility to responsible entities in determining the best way to identify anomalous activity to a high-level of confidence, so long as the methods ensure: (1) logging of network traffic . . . (2) maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation, and (3) maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures . . .. FERC Order No. 887, at ¶ 80.

While recognizing this need for flexibility, however, Texas RE is concerned that some of the identified measures, such as a list of detection events or INSM configuration settings, may be too vague to provide meaningful evidence that the detection of anomalous network activity security objective is being meaningfully performed. To prevent this, Texas RE suggests inserting language in the measures that clarify that, at a minimum, data collection methods must be of sufficient data fidelity to draw meaningful conclusions and support incident investigation consistent with the language in FERC Order No. 887.

Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	

The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards is ambiguous on if a baseline is required in its current version.

Likes 0	
Dislikes 0	

Response

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

A clear definition of “anomalous” is needed in order to determine compliance. For example, in Generation, certain activity that may take place during an outage may not be considered “anomalous” and would not invoke CIP-008. Also, the wording "Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action." is of a concern. It is vague and lets entities make their own decisions, which could be seen as audit bait when being audited.

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 concerns in relation to the use of term "anomalous activity" as this could be varied in terms of application and usage and is left to the entities to interpret.

BC Hydro also has concerns over the expected evidence needed for "documentation of responses to detected anomalies" per Measure M1 to meet Part R1.3., which seems to indicate that proof that all detections were responded to regardless whether they were false positives will be required, i.e. proving the negative on all anomalies detected. Due to this BC Hydro has concerns over a very high amount of data which needs to be analyzed and documented based on Requirement R1 Part R1.3 as drafted.

BC Hydro recommends to make the scope concise in the language of CIP-015 Requirement R1 Part R1.3, and add example scenarios and use-cases in the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA agres with EEI comments about the word "appropriate" being too open for interpretation.	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with EEI comments below: "The term “appropriate” is a subjective term. We propose the following revision: “Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2" This language is similar to the language used in CIP-008-6. Additionally, as described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy believes that the “appropriate action” language is too subjective and should be removed. We understand that in the process of tuning INSM implementations may generate lots of alerts, with the majority being false positives. We think that there is a way to tie the language to CIP-008 without arbitrarily treating each alert as an attempt to compromise. We suggest “Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine if a CIP-008 Cyber Security Incident response plan activation is required as a response.	

Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	

AES agrees that Part R1.3 provides entities the flexibility to evaluate and determine appropriate action. However, from the point where a determination is made and going forward, all related activities should be driven by existing Requirements in CIP-008.

AES also agrees with EEI comment below

EEI appreciates the SDT's revisions to allow Registered Entities to have flexibility to evaluate activity detected in Part 1.2 to determine appropriate action, however, the term "appropriate" is a subjective term. We propose the following revision: "Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2" This language is similar to the language used in CIP-008-6.

Additionally, as described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).

Likes 0	
Dislikes 0	
Response	

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Since Part 1.3 requires two separate actions, SPP recommends the following edit to the proposed language in R1, Part 1.3 (I.e., “change the word “to” to “and”): Implement one or more method(s) to evaluate activity detected in Part 1.2 and determine appropriate action.	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
The way the measures for Part 1.3 are written, it appears entities could select just one. Was this the intent of the DT? Consider revising to clarify that documentation is needed for evaluating and responding to anomalous or unauthorized network activity and an escalation process linking it to CIP-008.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
BPA believes there is still room for clarification to revise “anomalous network activity” to “anomalous conditions”. Network conditions can include lack of activity or states.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI’s comments: EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
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	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
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	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
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	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
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	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
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	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
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	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
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	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 6.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
While the measures do provide guidance, the requirement language should be clear in the intent. Texas RE recommends the following language to clarify the intent of Requirement Part 1.3: R1.3 Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action, up to and including identifying the anomalous network activity as a Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer	No
Document Name	

Comment

AES agrees with protecting INSM data from being inadvertently deleted or modified. However, we do not want the categorization or treatment of INSM data be conflated with or mistaken for BCSI. The two types of information must be treated as two separate and discrete types of information.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	

Comment

Duke Energy sees additional opportunities for clarification in R2. We are concerned that R2 is redundant for entities who will classify their INSM systems as EACMs, and that the flexibility in INSM system classification is not clear. We propose “Responsible Entity with an INSM system not classified as an EACM shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	No
Document Name	

Comment

Black Hills Corporation seeks clarification on how this Requirement R2 differs from the existing CIP-011 language regarding data protection, as we would like to see a standard that does not duplicate or conflict with existing CIP requirement language.

Black Hills Corporation also agrees with the comments from EEI: EEI proposes the following revision to CIP-015-1 R2:

Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (*remove*: , except during CIP Exceptional Circumstances).

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. The standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data.

Furthermore, Cogentrix proposes that ISNM data be specifically added as an item for CIP-011 classification as BCSI; as a result, this requirement is not needed.

Likes 0	
Dislikes 0	

Response

C. A. Campbell - LS Power Development, LLC - 5

Answer	No
Document Name	

Comment

The way in which this requirement reads there are CIP-012 overtones. Protecting data against the risks of 'unauthorized deletion or modification' is too close to the goal/objective of CIP-012, creating confusion and cross-over.

Likes 0	
Dislikes 0	

Response

Robert Follini - Avista - Avista Corporation - 3

Answer	No
Document Name	

Comment

Avista agree with EEI comments

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees with the feedback by EEI.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment
NEE support's EEI's comment(s): EEI proposes the following revision to CIP-015-1 R2: Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement. EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment
Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	

Comment
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #7.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No, there are a variety of of events, logs and other evidence based output that is generated by other CIP standards that don't require this level of protection. This appears to be overreaching in the protection of data that is beyond the protection of the BCS requirements.

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
It is not clear if the Requirement R2 is expecting both detection of unauthorized access and/or changes along with protection mechanisms to prevent unauthorized access or if the entity can choose what combination of controls is appropriate to them based on their security risk tolerance.	

BC Hydro recommends to provide clarity in the Requirement R2 to remove ambiguity and scope these accurately. BC Hydro also notes that although Technical Rationale provides examples of guidance it is not an ERO endorsed compliance guidance document. Auditors may chose to adhere to certain aspects from Technical Rationale and choose to leave others.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

EEI proposes the following revision to CIP-015-1 R2:

Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

See comments submitted by the Edison Electric Institute.

Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. NPCC RSC is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data."	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Does this suggest that the RE maintain the evidence? Why? For how long? What is the purpose and intent of this requirement? Could CIP-004 (access), CIP-005 (vendor access) or CIP-011 (BCSI protections) be leveraged for this purpose? Clarification is needes as it is not clear what the purpose and intent of this requirement is.	

What does "To mitigate the risk of unauthorized deletion or modification" mean? Again, shouldn't CIP-004 R4 and CIP-011 address this? Also, do the individuals who have the access, be the ones authorized to have the access. One concern is when vendors who have this access, and how would an entity monitor for such activity?

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI proposes the following revision to CIP-015-1 R2:

"Responsible Entity shall implement***, except during CIP Exceptional Circumstances,*** one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification."

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale:

BHE seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to

apply BCSI protections to INSM systems and its components. BHE seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6

Answer	No
Document Name	

Comment

Seminole agrees the EEI

EEI Response:

Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes there is an operational concern that logs should be set to over-write rather than causing a full disk stop condition. This may be a higher priority than keeping all logs, as the proliferation of security event logs, in itself, is an indicator of an issue that can feed into response activities.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	

The protection of the data does not need additional standards since a risk has not been identified that this newly created data element is subject to. Why would this data be subject to risk of unauthorized deletion or modification compared to other security logs or data?

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

The NAGF recommends placing the following statement "except during CIP Exceptional Circumstances" after the word implement which specifies the action for the phrase rather than a general statement.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale:

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Keele - Entergy - 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	
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	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO 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	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
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 Collaborators	
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	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. TFIST is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data	

Likes 0	
Dislikes 0	
Response	

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	

Comment

Seminole Agrees with the comments from MRO NSRF

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	2023-03_Comment_Form_MRO_NSRF_20240313_Final.docx
Comment	

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests **eliminating CIP-015 R3** and **adding a new sub part 1.4** a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	
Response	

Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Concerns with the language in R3. The amount of data to be collected and stored is extremely voluminous, which in turn is a very expensive administrative burden that does not provide additional security or reliability. Suggest modifying the language for R1.2 and R1.3 to reflect limiting the data retained to network communications and other related data as part of the investigated alert.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows: “Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail for at least ninety days,** INSM data **evaluated** in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.” The choice for “ninety days” duration is meant to keep consistency with other CIP Standard log retention requirements.	
Likes 0	
Dislikes 0	
Response	

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

"Responsible Entity shall implement one or more documented process(es) to retain***, with sufficient detail and duration, INSM data evaluated in support of*** Requirement 1, Part 1.3 ***and determined by the Responsible Entity to be anomalous and require action***, except during CIP Exceptional Circumstances."

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The phrase "retain network communications data AND other metadata." This insinuates that entities may need full PCAP monitoring of an entire BCS and retaining entire conversations. This could require signifigant allocation of resources from entities, especially if storage is required for a signifigant amount of time. Entities should be able to establish retention requirements in their program for full PCAP if required to implement as this approach may not be cost effective for entities.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

It is unclear as to how to meet any objectives of this requirement. Again, the word anomalous needs clarification. The way the requirement is written is still vague in determining how long to retain network communications data and meta data collected with sufficient detail and duration to support the analysis. The technical guidelines has more in-depth information on what should and can be the length of time. However, as we all know, auditors will be auditing to the Standard and requirements and not the technical rational. Maybe include additional information in the measures section?

Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	No
Document Name	
Comment	
The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. The data to be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System. *Consider:* *R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.*	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Georgia System Operations Corporation supports ACES comments: "ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc."

Likes 0	
Dislikes 0	

Response

Hillary Creurer - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Minnesota Power supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments:

"R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. NPCC RSC is unclear on what "sufficient detail and duration" means and if these words are necessary."

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	No
Document Name	

Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP asks that the SDT provide additional clarity around (i) what is a reasonable duration for network communications data and metadata retention, and what is defined as network communications data and metadat	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
It is unclear on how long the data needs to be retained. Suggest including a clear timeline minimum 90 days to match with CIP-007 R4.3 event Log retention	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	

EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

"Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during 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

BC Hydro has concerns about the extensive data volume and high costs associated with Requirement R3 per the current language. BC Hydro suggests limiting retained data to network communications and relevant information linked to investigated alerts only. A full capture of network data poses excessive burdens in terms of cost and sustainment and does not contribute extensively in enhancing security or reliability for the Bulk Electric System. BC Hydro recommends that the drafting team narrow the scope of INSM (Internal Network Security Monitoring) data to only Attempt to Compromises and reportable Cyber Security Incidents only in line with CIP-008 requirements.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail for at least ninety days,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.” The choice for “ninety days” duration is meant to keep consistency with other CIP Standard log retention requirements.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA agrees with AES statement.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
Dominion Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
AEPC has signed on to ACES comments: ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment
NST believes R3 should clarify it is left to Registered Entities to decide what collected data should be retained and for how long. We suggest, "Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration, *as determined by the Responsible Entity,* to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances."

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The SRC recommends that the standard be revised to provide additional clarity regarding the extent of a Responsible Entity's ability to define and determine what data (particularly metadata) needs to be retained and the appropriate retention period. Without additional clarity, the SRC is concerned that Requirement R3 could be construed to require entities to retain large amounts of data for the full duration of the three-year evidence retention period applicable to CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE support's EEI's comment(s): EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows: "Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	

AZPS agrees with EEI's concerns regarding the proposed language for CIP-015-1 R3. Potential ambiguity in the current draft of data collection requirements may lead to interpretations which require significant data collection and storage. AZPS supports the following revised language:

"Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees with the feedback by EEI.

Likes 0	
Dislikes 0	

Response

Robert Follini - Avista - Avista Corporation - 3

Answer	No
Document Name	

Comment

Avista agrees with EEI's comment -- EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications.

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 6

Answer	No

Document Name	
Comment	

"***R3*** *Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected* ***with sufficient detail and duration*** *to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances*."

The bolded part ("with sufficient detail and duration") is unquantifiable and can potentially be too subjective. LDWP would recommend specific criteria or additional technical guidance be included for what "sufficient detail and duration" entails.

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	

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	
Response	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. This brings the question of what "sufficient detail and duration" means and are these words are necessary? Further, other approved CIP standards offer specific data retention periods. Cogentrix does not believe this ambiguity is helpful to the objective and the DT should specify a timeframe to help clarify entity expectations and introduce consistency in application.

Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

"Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** (*remove:* network communications data and other meta data) INSM data (*remove*: collected with sufficient detail and duration) **evaluated** (*remove:* to support the analysis) in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."

Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	

The proposed language in R1 1.3 and R3 is ambiguous and should be revised. Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.

Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State agrees with the comments below:

AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive.

AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

*1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.*

*1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred.***

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

***1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall* initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.**

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	

Comment

Duke Energy suggests additional clarification on the retention expectation for R3 and removal of the language “sufficient detail and duration”. We would suggest this alternative language “Responsible Entity shall implement one or more documented process(es) to retain network communications data collected to complete the analysis in Requirement R1, Part 1.3 and to execute their Cyber Security Incident response plan where required.

Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Is there an intended difference between “INSM data collected” as referenced in R2 when compared to “network communications data and other meta data collected” as referenced in R3? If this is the same thing, ATC supports the intent of the requirement, but requests consideration of using consistent terminology for clarity.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12. **This will likely be more of a function of cost versus want. Depending on number of alerts and need to keep for entire audit period.**	

Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
PNMR agrees with R3, but to more closely align with R2, which states entities must protect INSM Data, PNMR believes the language of R3 should read: “Responsible Entity shall implement one or more documented process(es) to retain INSM data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	

The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA recommends that a suggested minimum retention parameter be included in the Technical Rationale. BPA believes this would be in alignment with language cited in CIP-007 R4, 90-day event log retentions.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
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	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - 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	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
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	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. TFIST is unclear on what “sufficient detail and duration” mean and if these words are necessary.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned that not establishing guidelines or thresholds for minimum retention periods, this requirement would be a challenge to comply with, audit, and enforce consistently. Texas RE notes that FERC Order No. 887 specifically identifies the need to “maintain . . . logs, and other data collected, regarding network traffic” as key security objective for the implementation of an effective INSM program. Failure to maintain evidence of the collection of log data renders this security objective essentially unenforceable. Texas RE concedes that a blanket requirement to retain logs may not be appropriate to meet this security objective. For example, from a storage perspective it would be very expensive to require network traffic of full system backups to be stored for 90 days. Likewise, from a threat perspective this is known and expected traffic and would be of minimal benefit to store. As such, Texas RE recommends adding language to the requirement for Registered Entities to explicitly define types of traffic that will not be required to be retained. Registered Entities could write into their program that expected traffic will be excluded from storage and retention requirements. However, this expectation should be clear from the requirement language itself, and the burden placed on entities to carefully define and demonstrate they are accomplishing the FERC-mandated security objective to retain maintain sufficient logs regarding network traffic so that can detect anomalous events and effectively demonstrate compliance with that expectation.	
Likes 0	
Dislikes 0	
Response	

Ruchi Shah - AES - AES Corporation - 5	
Answer	
Document Name	
Comment	

AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive.

AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

*1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.*

*1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred.***

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

***1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall* initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.**

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Option 2:

If the drafting team does not agree with Option 1, AES suggests modifying R3 to read:

R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration ***collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3****, except during CIP Exceptional Circumstances.*

Likes 0	
Dislikes 0	

Response

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.	
Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
No, Southern Indiana Gas & Electric (SIGE) does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
No, CenterPoint Energy Houston Electric (CEHE) does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not	

interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. CEHE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.. The undertaking will demand significant effort, substantial capital investment and additional staffing.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA reiterates its comments from the previous comment period regarding the proposed implementation plan timeline.

BPA's previous comments: "After reviewing the new requirement language in CIP-015-1, BPA believes more time will be required to implement an INSM program. This takes into consideration the initial effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'"

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
This Standard's implementation as drafted can be very time and cost intensive due to language in R3 as commented in response to Question #8 above.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
SRP would need for the questions above to be answered and the standard to be clearer before we can make a determination on a timeline. Currently the standard is written as a Subjective standard vs. an Objective standard and additional clarity would be needed.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 Implementation Plan timing.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
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 comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	

Response
Robert Blackney - Edison International - Southern California Edison Company - 1
Answer	Yes
Document Name	
Comment
See comments submitted by the Edison Electric Institute.
Likes 0	
Dislikes 0	
Response
Kinte Whitehead - Exelon - 3
Answer	Yes
Document Name	
Comment
Exelon is aliging with the EEI in response to this question.
Likes 0	
Dislikes 0	
Response
Daniel Gacek - Exelon - 1
Answer	Yes
Document Name	
Comment
Exelon supports the comments submitted by the EEI for this question.
Likes 0	
Dislikes 0	
Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
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: "NPCC RSC agrees with the implementation plan."	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	

Answer	Yes
Document Name	
Comment	
Georgia System Operations Corporation supports ACES comments: "While ACES does not oppose a 36 month implementation plan, ACES believes the INSM OT industry and ERO lack sufficient SMEs to get this implemented fully by all entities across the ERO in 36 months. ACES feels there needs to be an extension provision in the implementation plan."	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Constellation feels strongly that more than 18 calendar months is needed for implementation.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
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	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Keele - Entergy - 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	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
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	

Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
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

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

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	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 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 Collaborators	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC defers to the comments by the applicable entites on the Implementation Plan	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
Was not discussed on 3/7/2024 meeting.	
Likes 0	
Dislikes 0	
Response	

10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

More clarity within the requirements is needed to determine cost-effectiveness of needed controls.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

This standard will require substantial investments in infrastructure to accomplish the monitoring objects, as well as additional personnel to provide adequate monitoring coverage and support of these systems and associated compliance requirements. A more flexible standard that incorporates monitoring from the endpoint would align more closely with existing security monitoring initiatives. Cost-effectiveness is not possible to determine with the limited clarifications at this time. More information is needed.

Likes 0	

Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect

Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

Georgia System Operations Corporation supports ACES comments:

"ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

The risk needing to be reduced or closed
How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective
How much vendors will increase prices due to INSM requirements
Implementation capital cost
Annual Operation and Maintenance cost
How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan

Market analysis of SMEs needed to manage INSM as required"	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks the SDT to consider the potential cost that may arise from the scope of these requirements. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, managing, and storing of all INSM data and metadata for any length of time will be substantial	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Please refer to comments in Question #8 above.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.	

Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA would need further analysis to detertime the cost effecivness of the proposed standard.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

AEPC has signed on to ACES comments:

ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

1. The risk needing to be reduced or closed
2. How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective
3. How much vendors will increase prices due to INSM requirements
4. Implementation capital cost

5. Annual Operation and Maintenance cost

6. How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan

7. Market analysis of SMEs needed to manage INSM as required

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.

Likes 0	
Dislikes 0	

Response

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer	No
Document Name	

Comment

SMECO agrees with ACES comments:

ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The SRC is concerned that the issues identified in its responses to questions 4 and 8 could materially impact the cost of meeting the underlying reliability goal and FERC directives. Specifically, if Requirement R1 is not clarified as discussed in the SRC's response to question 4, Responsible Entities may have to incur costs to upgrade or replace equipment that uses nonstandard communication protocols for which no effective INSM technology exists. If Requirement R3 is not clarified as discussed in the SRC's response to question 8, Responsible Entities may need to incur the costs of storing large quantities of data for the duration of the three-year CIP-015-1 evidence retention period.

Likes 0	
Dislikes 0	

Response

Wendy Kalidass - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications 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. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.

Likes 0	
Dislikes 0	

Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Without further study the costs associated cannot be determined at this time.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E does not have any current way to judge the cost-effectiveness of these requirements until the modifications have been approved.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
No, without further study, CEHE believes the costs associated with the new requirements cannot be determined. Some substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	

Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
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	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
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	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter
Answer	
Document Name	
Comment
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.
Likes 0	
Dislikes 0	
Response
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5
Answer	
Document Name	
Comment
Was not discussed on 3/7/2024 meeting.
Likes 0	
Dislikes 0	
Response
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP
Answer	
Document Name	
Comment
WECC defers to the comments by the applicable entites on the Cost Effectiveness of the Standard.
Likes 0	
Dislikes 0	
Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST lacks the information necessary to comment on this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	

Document Name	
Comment	
BPA reiterates its comments from the previous comment period regarding cost-effectiveness. BPA's previous comments: BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
MRO NSRF has no comment on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	
Comment	
No. From a generation facility perspective, this would be a heavy lift and substantial cost burden. As indiciated on the INSM survey submitted last year, owners with multiple assets (especially generaiton) do not have baked-in cost recovery mechanisms. LS Power Development recommends referring to survey responses, specifically those from GO/GOPs. IT/OT support services at the plant level is a relatively newer initiative, and network infrastructure requirements per CIP-015 (though practical and good cyber security practice) are still cripling cost-wise. Other than performing a study to realize the actual risks to generation facilities, there presently isn't sufficient justificaiton.	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
Will need to research a solution to see if it is cost effective.	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
Will need to research a solution to see if it is cost effective.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	

11. Please provide any additional comments for the DT to consider, if desired.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 DT for their consideration of the industry's input which included the creation of CIP-015 and the modifications from the last ballot.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation recommends adding the following definition to the NERC Glossary of Terms:

Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.

Reclamation appreciates the DT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the DT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.

Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	

Black Hills Corporation repeats EEI's comments: EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).

Likes 0	
Dislikes 0	
Response	

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	

Cogentrix recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards.

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	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	
Comment	
Thank you so much for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
Generator Owner was left out of applicability, should be re-added.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
While TVA appreciates the flexibility afforded by the proposed risk-based language, additional clarity or assurance regarding how the CEA will approach auditing and determine sufficiency would be helpful.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE support's EEI's comment(s): EI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST respectfully offers the following comments/suggestions on the Technical Rationale document: > The document includes several statements about compliance that seem to have been written as statements of fact. Three examples, numbered for reference purposes, are: (1) "Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R1, Part 1.2 or 1.3." (2) "Short periods of reduced visibility should not justify a potential non-compliance finding, especially when other cybersecurity monitoring is in place." (3)"Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2." NST believes it is beyond the SDT's purview to make such assertions, and we therefore recommend they be reworded to clarify they only represent STD opinions. With regard to statement (1) and the idea of suspending INMS monitoring or suppressing alerts while maintenance and/or system upgrade activities are in progress, we believe a better approach to allowing an Entity to do this without risking instances of non-compliance would be to add exception language to Requirement R1 that allows for this. > NST believes the paragraph titled, "External Networks" is confusing at best. We presume the STD's intent is to encourage Entities to implement INSM in high-value networks outside of ESP. While we are inclined to agree it might be worthwhile, we believe that by virtue of being beyond the scope of CIP-015, it should be omitted.	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF notes that the phrase “detecting anomalous or unauthorized activity” in section R1 is of concern as the use of the word “unauthorized” implies a program to authorize network level activity within the ESP. As a network level monitoring standard, entities will need additional context of system monitoring (such as logs) or other data (e.g., work orders for adding new devices to a network) to determine “unauthorized activity” from a detected anomaly. Also, with an “or” between them, an entity can monitor for only unauthorized and ignore anomalous traffic. As unauthorized activity is a subset of anomalous activity, we suggest striking “or unauthorized”. It is also noted that requirement part 1.2 only mentions “anomalous network activity” and this would align it with the remainder of the sub-requirements.	
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
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer
Document Name
Comment
Texas RE reiterates its concerns that this standard would be a challenge to audit and enforce consistently. In Requirement R1, the phrase “based on network security risk(s)” is vague and does not include criteria establishing the network security risks, which could lead to Parts 1.2 and 1.3 not being relevant. Second, Requirement R3 does not specify how an entity should determine the retention periods, thus leading to a vague requirement.
Likes 0
Dislikes 0
Response
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC
Answer
Document Name
Comment
SMUD recommends the Standards Drafting Team (SDT) change the language in Requirement R1, Part 1.2 so that it is consistent with Requirement R1. Requirement R1 states “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of *detecting anomalous or unauthorized network activity*.” Requirement R1, Part 1.2 states “Implement one or more method(s) to *detect anomalous network activity* using the data collected at locations identified in Part 1.1.” Although this inconsistency is minor, the SDT has the opportunity to make the change now and improve the quality of this Standard. This language change is non-substantive and could be made for the final ballot posting.
Likes 0
Dislikes 0
Response
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer	
Document Name	
Comment	
We support TFIST comments	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC appreciates the SDT addressing ATC's comments from the previous round while maintaining and objective approach and commensurate flexibility in the requirement language.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	
Document Name	
Comment	
EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	

Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	
Document Name	
Comment	
Constellation concurs with NAGF's comments. In addition, Constellation wants the DT to provide further guidance on anomalous or for it to be defined.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	

ACES would like to thank the SDT for all their hard work and allowing us to provide feedback	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "NPCC RSC recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards."	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	

ITC supports EEI's comments on this project.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	
Document Name	

Comment

The Technical rational is well written with a lot of detail, however this document from my understanding will not be part of the audit. I would like to see more in the measures, as a high-level for better understanding. Leaving it up to the entities, may still become audit bait, unless each entity writes up their rational. The standard is written a Subjective standard vs. an objective standard, this leaves it up to the entity to decide what to audit it on.

The definition anomalous activity needs to be defined; Baseline needs to be defined. Overall, there needs to be a standardized approach for auditing this requirement.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment	
The VSLs are too high for R2/R3 compared to R1. Maintaining full logs that only went back 82 days (vs 90) is potentially as or more severe than having a program in place at all (R1). The drafting team should consider a higher VSL for R1 as compared to a lower VSL for R2 & R3 as currently written.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	

Kelly Bertholet – Manitoba Hydro

Question 1 -Yes
Comments: Manitoba Hydro supports this change as the previous conditional inclusions were a source of confusion for many.

Question 2 -Yes

Question 3 -Yes
Comments: Manitoba Hydro supports this clear direction.

Question 4 -Yes

Question 5 -Yes
Comments: Manitoba Hydro agrees with this approach, which is clear in its intent. However, there is a concern that the phrase “detecting anomalous or unauthorized network activity” in R1 does not align well with Parts 1.2 and 1.3. We recommend striking “or unauthorized” in R1 to better align with the rest of the standard and avoid confusion as to whether this criteria is “one or the other” or referring to detecting both anomalous and unauthorized network activity. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.

Question 6 -Yes

Question 7 -Yes

Question 8 -No

Comments: Manitoba Hydro is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle could be extremely voluminous and overly expensive. Manitoba Hydro believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, Manitoba Hydro suggests modifying R3:

Responsible Entity shall implement one or more documented process(es) to retain meta data collected to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.

Question 9 -Yes

Question 10 -Yes

Question 11 – Comments: Generator Owner was left out of applicability, should be re-added.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-03 Internal Network Security Monitoring | Draft 1 of CIP-015-1
Comment Period Start Date:	2/27/2024
Comment Period End Date:	3/18/2024
Associated Ballot(s):	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 IN 1 ST Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 73 sets of responses, including comments from approximately 160 different people from approximately 102 companies representing 7 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, Soo Jin Kim (via email) or at (404) 446-9742.

Questions

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

Project 2023-03 – INSM received unanimous support for the Drafting Team's (DT's) decision to continue the project without the inclusion of EACM and PACS outside of the ESP in the scope of proposed Reliability Standard CIP-015-1.

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

Project 2023-03 – INSM received overwhelming supported from industry to create a new objective-based standard (proposed Reliability Standard CIP-015-1) as opposed to revising Reliability Standard CIP-007-X with a new Requirement R6 and/or revising other existing CIP reliability standards.

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity's ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The Project 2023-03 DT appreciates the valuable feedback received regarding Question 3. To address the feedback received, the DT modified Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks

protected by the ESP that are the focus of Requirement R1, and 2) to ensure all requirement Parts are supported by the language in Requirement R1.

Additionally, the DT removed the words "increased the probability of" from Requirement R1. Moreover, recognizing that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale that can be leveraged to develop an INSM.

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The Project 2023-03 DT appreciates the valuable feedback received regarding Question 4. The DT made modifications to Requirement R1 Part 1.1. to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than alternative language proposed by several commenters. Moreover, the DT received comments that referenced "locations" could be confused with geographic locations, so the DT modified "network data locations and methods" with "network data feed(s)".

The DT reviewed the SAR, and with respect to the reference to monitor network activity including software, it is the opinion of the DT that the network data related to software will be included in the elements contained in Requirement R1, Part 1.1.

5. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the

requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT considered whether or not to create a NERC Glossary term for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT felt "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

While CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT determined that most entities are logging events at the Cyber Asset level in a security information and event management (SIEM) system. Additionally, the SIEM may be used for analysis and retention of those host-level events to meet CIP-007-6, Requirement R4 and allow for detection of login attempts and malicious code on those Cyber Assets.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

The DT agrees that striking "or unauthorized" in Requirement R1 better aligns with the other requirements in the proposed standard and updated Requirement R1 for Draft 2 of proposed Reliability Standard CIP-015-1.

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT considered whether or not to create a NERC Glossary term for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT felt "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

The DT removed "appropriate action" and replaced it with "further action(s)". Requirement 1, Part 1.3 was updated for Draft 2 to: "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after the evaluation in Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's CIP-008 incident response process(es) for further investigation.

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT has updated the Technical Rationale document for clarity on Requirement R2. Additionally, the DT has also created a FAQ document for this project that states, "Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network."

Requirement R2 has been revised to: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification."

The DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

Data protection in proposed Reliability Standard CIP-015-1, Requirement R2, is intended to protect the data from being altered or removed by an advisory intended to cover their tracks. BCSI protection as defined in the CMEP guide and CIP-011 is to protect against data or information that could be used to gain unauthorized access to a BES Cyber System.

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT made the following changes:

- Requirement R3 was revised to the following:

  "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]"

- The DT added a note to R3 stating:

  "Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."

- The DT is hesitant to have potential overlap with an entity's existing CIP-008 processes. The DT altered Requirement R1, Part 1.3 to state:

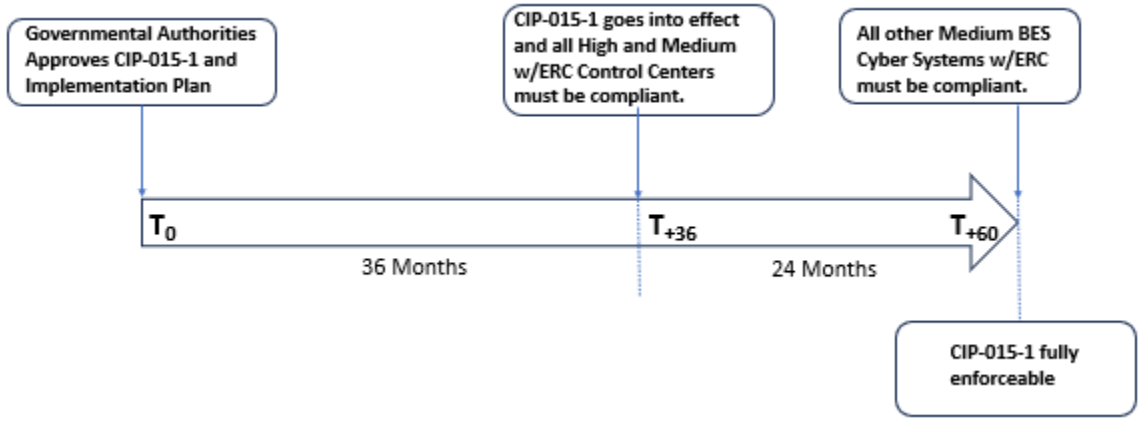
"Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s)."

The implication is that anomalous activity will require a response that could range from tuning software, if the activity is noise, to escalating into the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations, which may be more challenging to implement.



10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cybersecurity Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

11. Please provide any additional comments for the DT to consider, if desired.

Summary Response:

Generator Owners have been included in Section 4 Applicability. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS)."

The DT revised Requirement R1 and removed "or unauthorized" from the requirement.
For R1, the current draft has the language "Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications…" the DT believes that this will allow entities to customize their monitoring locations and to have a documented rationale for why those locations were chosen for audit defense.

The DT considered whether or not to create a NERC Glossary term for "anomalous." After reviewing the Merriam-Webster dictionary definition, the DT felt "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

Requirement R3 has been revised to the following:

"Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."

The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.

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
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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO

					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities- Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC

Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	1	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
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
					John Nierenberg	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
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC

					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Jason Procuniar	Buckeye Power, Inc.	4	RF
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE
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
					Mark Garza	FirstEnergy- FirstEnergy	1,3,4,5,6	RF

					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
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
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6			Micah Runner	Black Hills Corporation	1	WECC

				Black Hills Corporation - All Segments	Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	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
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
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
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
					Gary Dollins	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC

Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
Tony Gott	KAMO Electric Cooperative	3	SERC
Micah Breedlove	KAMO Electric Cooperative	1	SERC
Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
Jarrod Murdaugh	Sho-Me Power Electric Cooperative	3	SERC

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports this change, and thanks the Drafting Team for their careful consideration of the scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 supports the modifications.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
A PCA is within an ESP, the question is worded incorrectly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
The term "PCA devices outside of the ESP" appears to contradict the NERC definition of PCA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

MRO NSRF supports this change, as the previous conditional inclusions were a source of confusion for many.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA endorses removing "EACMS, PACS, and PCA devices" from the requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company appreciates the change in scope for this version of the standard. The original scoping in the standard for individual systems outside of a defined ESP in requirements intended at a network (and not system) level is problematic. If the intent of the standard included system level monitoring rather than network monitoring only, how to scope such requirements to individual systems would be clearer. We appreciate the clearer scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments for all questions	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI's comments.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments for all questions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST recommends that, for the sake of consistency with CIP-007, CIP-015's scope include BES Cyber Assets and any associated PCAs (which exist only inside ESPs).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
WECC agrees with not including EACMS, PACS and PCAs outside ESP as it would not be consistent with the applicable systems scope of the SAR. However, we note that any scope of 'PCA devices outside of the ESP' is not supported by the definition of a PCA – 'One or more Cyber Assets connected using a routable protocol **within or on an Electronic Security Perimeter** that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.'	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Clay Walker - Cleco Corporation - 1,3,5,6 – SERC	
Answer	Yes

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Teresa Krabe - Lower Colorado River Authority – 5	
Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

BHE agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	
A PCA is within an ESP and the question is worded incorrectly	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Glen Farmer - Avista - Avista Corporation – 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Alain Mukama - Hydro One Networks, Inc. – 1	
Answer	Yes
Document Name	
Comment	
Don't see the issue, but the final requirement verbiage should be clear on the Applicable System(s)/ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	

Kinte Whitehead - Exelon – 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon – 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	

Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "A PCA is within an ESP and the question is worded incorrectly. "	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1. Please see responses to NPCC RSC's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
PCA devices do not sit outside of the ESP. Please clarify if the DT intention is to exclude PCA devices (in the ESP) or to simply exclude EACMS and PACS (outside of the ESP).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Ruchi Shah - AES - AES Corporation – 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy – 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC – 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	
Document Name	
Comment	
SUPPORTING EEI COMMENTS ON ALL QUESTIONS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
SRP could support the creation of an entirely new standard once we understand the definition of “objective-based”. Please clarify “objective-based” or explain what it actually means.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT vetted the comment requesting clarification of “objective-based”. The DT believes the current revision of proposed Reliability Standard CIP-015 addresses this comment. The DT afforded entities’ flexibility in using various INSM methodologies and technologies, which are “objective-based”. Additionally, the DT updated the Technical Rationale document to reflect additional methods of analysis and to ensure that various tools can be used to comply with the newly drafted CIP-015 standard.	
Alain Mukama - Hydro One Networks, Inc. – 1	
Answer	No
Document Name	
Comment	

If INSM not going to be in CIP-007 R6 and creating CIP-015 for INSM, why not move CIP-007 R4 Security Event Monitoring also to this new CIP-015?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The requirements of CIP-007, Requirement R4 applies to systems management, and CIP-015-1 applies to the network security monitoring.	
Gail Golden - Entergy - Entergy Services, Inc. – 5	
Answer	No
Document Name	
Comment	
This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches. Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives.	

CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.	
James Keele - Entergy – 3	
Answer	No
Document Name	
Comment	
This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches. Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives. CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp – 6	
Answer	Yes

Document Name	
Comment	
BHE agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. – 1	
Answer	Yes/
Document Name	
Comment	

Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments on this project.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon – 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon – 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. Please see responses to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	

While TVA understands the challenges to updating CIP-007 to include internal network security monitoring we believe that these changes should be included within existing monitoring requirements or those requirements, mainly CIP-007 R4, be moved to CIP-015 as well. INSM should be an extension of the existing required cybersecurity monitoring program, not a new program. By combining the two efforts some of the same requirements between CIP-007 R4 and the INSM components in CIP-015 may be used. Additionally, if the scope of the standard is expanded to Low systems in the future this will make it easier to apply the full monitoring program that would be needed.

Moving the proposed monitoring requirements to CIP-015 removes these obligations from the scope of the existing CIP-003 Cyber Security Policy – suggest consider revising CIP-003 to include CIP-015 in Cyber Security Policy.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The requirements of CIP-007, Requirement R4 applies to systems management, and proposed Reliability Standard CIP-015-1 applies to network security monitoring. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches.

Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives. CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 supports the modifications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
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	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 2	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports this change and agrees that a new standard is the best approach to incorporating the INSM revisions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity's ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES supports EEI comment below EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	

Tri-State agrees with EEI comments below:

"EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses to EEI's Comments.

Wendy Kalidass - U.S. Bureau of Reclamation – 5

Answer	No
Document Name	

Comment

Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. There are many approaches and methods to achieve the security objectives of this requirement and a "one-size-fits-all" approach might not align with all current and future network environments. The DT has provided additional context in the Technical Rationale that can be leveraged to develop an INSM and focusing on specific risks for the Responsible Entity.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous (*remove:* or unauthorized) network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. Suggest R1 be rewritten to state that the standard requires monitoring of the network within an ESP to include all systems that are connected therein, whether permanent or temporarily (such as Transient Cyber Asset).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
FirstEnergy believes clear separation of where CIP-005 ends and where CIP-015-1 begins in terms of enforcement would benefit the scope of CIP-015-1. Since 'internal network security monitoring' will not be a defined term and Technical Rationale explanation are not part of the enforceable Requirement, FE asks the Drafting Team to more clearly identify their technical rationale in the standard so as to "help" Responsible Entities define that term for themselves, understanding the baseline knowledge of NERC and its Regional Entities. Finally, FirstEnergy suggest removal of the conjunctive “or unauthorized” in the opening sentence of R1. The use of the term “unauthorized” hints at this should include some sort of authorization process paperchase for every network communication which is impractical and not related to potentially malicious network traffic.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the feedback by EEI. In addition, Southern has concerns with the phrase “increase the probability of detection” as the stated objective. Southern agrees that such a concept is necessary to prevent R1 from requiring 100% perfection of detection which no tool can guarantee. As this phrase is the core of the requirement's objective and what it is to accomplish, the focus is on an "increase" in probability and thus how your process accomplishes this increase, rather than whether the entity has implemented a process that can meet 1.1 to 1.3. A suggestion is to replace the phrase with “provide the capability of detection” or similar phrasing that is a far more binary judgment to make (did the entity implement a process to provide detection capability to meet all the requirement parts) and still avoids the 100% perfect detection of every anomaly issue. Therefore, if minimal change to R1 is required, we suggest the following (though we have a further suggestion of a more substantive change for consideration in Q4): Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability **provide the capability** of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's Comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	No
Document Name	
Comment	
NEE support's EEI's comment(s): EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
David Jendras Sr - Ameren - Ameren Services – 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

SMUD agrees with the comments submitted by Tacoma Power, and that the suggested language change to R1 is non-substantive and could be made for the final ballot posting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to Tacoma Power's comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	

Project 2016-02 modified the concept of an EPS to include Zero-Trust architectures, where there is no “inside” or “outside” an ESP, but rather relies on the idea of “protected by an ESP.” Tacoma Power Suggests the following language for CIP-015 R1: “Implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) or a medium impact BCS with External Routable Connectivity (ERC), **protected by an ESP**, to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]” Tacoma Power thinks the language change to R1 is non-substantive and could be made for the final ballot posting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's Comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
BHE appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows: Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	

EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response to EEI's comments.

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

See comments submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses to EEI's Comments.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	
Comment	
Clarity is required if INMS requirement is also applied to EACMS/PACS/PCA within ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. There are many approaches and methods to achieve the security objectives of this requirement and a “one-size-fits-all” approach might not align with all current and future network environments. We provided additional context in the Technical Rationale that can be leveraged to develop an INSM.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI’s Comments.	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	

OPG supports NPCC Regional Standards Committee's comments: "The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. NPCC RSC proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to NPCC RSC's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

SRP feels that there are no methods to measure compliance as the standard is stated. We ask to provide guidance as to what is required as evidence. Should detection be continuous, or is periodic detection permissible? Also, there is no timeline as to how often detection and evaluation should be performed (In real time? Every 15 minutes? Every 15 months?). The standard does not make it clear of the word "baseline" is. Perhaps, the "definition" or the expectation of what the baseline is should be in the measures section. The technical rationale "definition" of a baseline is more clearly defined under Detection Methods "Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.". However, we did not see any reference to what is in the methods for this wording.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. Numerous comments were received expressing support for providing flexibility to Responsible Entities to develop their programs without having specific timelines and obligations that may not align to the operations of all Responsible Entities. We provided details in the Technical Rationale that can be used to support the INSM programs for the Responsible Entities. Additionally, the DT updated the Technical Rationale with additional language to clarify the word “baseline” when used to describe anomaly detection technology.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
There is not a definition of "Network" in network security monitoring. While our *understanding* is that this standard is focused on network traffic monitoring, it is not explicit and, therefore, could be interpreted in multiple ways (EDR vs East/West traffic monitoring vs full network traffic monitoring, for example).	
Likes 0	

Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

"Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of ***detecting anomalous network activity***. The documented process(es) shall include each of the applicable requirement parts."

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

BHE appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	

Seminole Agrees with the comments provided by EEI "EEI appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees that the parent requirement R1 of CIP-015-1 clearly addresses INSM within a Responsible Entity's ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent and supports the modifications.	
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 comments submitted by the MRO NERC Standards Review Forum.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF supports this clear direction.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Existing monitoring standards are prescriptive to specific locations and event types that are possible to be monitored through traditional log review and automated evaluation. R1 is vague in the specific requirements that must be included in a process. Anomalous network activity is not defined within the standard or the glossary. This is left up to interpretation of the entity and the auditors. In the measures "Architecture documents" is beyond what is required for Electronic Security Perimeter drawings in CIP-005. Request for drawings should be limited to	

inclusions of elements within required drawings in the standards. The current draft of the standard also only allows for internal IDS types of solutions with detection event capturing and review.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The Measure was updated to remove the term “architecture” from the language. The Technical Rationale provides additional information to aid the Responsible Entity in developing their INSM program.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
PNMR agrees with intent of R1 but suggests changing the language from “to increase the probability of detecting” to “… to detect anomalous or unauthorized network activity”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1. Based on the feedback the DT removed the words “increased the probability of” from Requirement R1.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the drafting team's efforts to be responsive to FERC Order No. 887. Texas RE is concerned, however, that the language in Requirement R1 does not lend to consistent application and would be a challenge to audit and enforce. Since the language in Requirement Part 1.1 does not establish a minimal level of acceptable monitoring or establish a maximum level of risk acceptance, an entity could determine that there are no network data collection locations and methods. If there are no network data collection locations and methods identified, Requirement Parts 1.2 and 1.3 would not be relevant.	

Texas RE recommends clarifying “network security risk(s)”. The SDT could consider including network security risk criteria similar to how CIP-002 includes impact rating criteria or establishing minimum security risks similar to how CIP-007 Requirement R4 requires logging a minimum of certain types of events.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity; including connection, devices, and network communications. In addition, the associated measure states that the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. TFIST proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	

Seminole agrees with comments from EEI

"EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: "Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications." EEI proposes modifications to the draft M1, Part 1.1 measures to: "Architecture documents or other documents detailing data collection location(s) and method(s); or"

Seminole also agrees with Comments from Entergy

" The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider all possible network data collection locations. For example, and entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.” If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.”

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see responses to EEI’s comments and Entergy’s comments.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
BHE appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language: "Identify network data collection **point(s)** based on the network security **threat(s) and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications." These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.	

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language.

In addition, the DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)".

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cybersecurity Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No

Document Name	
Comment	
M1 1.1 - The term "documented rationale" is very open and can be a place where professional opinions may differ. A registered entity may have one an effective approach to monitoring but an auditor may have a differing opinion. While flexibility has its pro's and con's, some entities may prefer to have a little more specificity of what's needed to guide both the entity and regional entity audit staff.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the proposed alternative language. The Technical Rationale provides additional insights for Requirement R1, Part 1.1.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
No objectives to measure compliance have been provided. Self-proclaimed compliance would not be auditable (based on RE perception, rather than auditors). It is very vague, there is no measurement to consider what is acceptable. The entity can say I am always in compliance. There is no clear definition on how and how long to save off the data. Also, how to obtain the level of monitoring in the requirement is vague. This will be subjective vs objective. In addition, R1 1.1 states to identify location "based on the network security risk(s)" but does not attempt	

to quantify specific risk or suggest which level of risk they're seeking to address. While entities can determine their own level of acceptable risk, this could lead to a wide range of outcomes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. There are many approaches that can be taken to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No

Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "The current R1.1 requirements could be interpreted that a "Network Security Risk" evaluation or assessment could be required under the standard. NPCC RSC suggest removing "Network Security Risk" or stating that INSM should be for monitored of the entire network per technical capability or assets "Network Security Risk" for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to NPCC RSC's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	

See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language: "Identify network data collection location(s) **point(s)** and method(s), based on the network security **threat(s)** risk(s) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications." These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM. We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the drafting team efforts and the opportunity to comment. The use of the 'risk-based' language in CIP-015 R1.1 is leaving it to the discretion of entities to determine which component poses higher or lower risks. This will leave it open to the auditor's interpretation and expectation instead of ensuring the scope is concise and clear under this requirement. BC Hydro recommends to define the parameters of these 'risks' to give clear direction to entities or specify the network components on which this requirement R1.1 applies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches can be taken to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No

Document Name	
Comment	
BHE requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language: "Identify network data collection location(s) **point(s)** and method(s), based on the network security risk(s) **identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications." We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. In addition, DT received comments that reference "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)". The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	

FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cybersecurity Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that instructing Entities to use a "risk-based approach" to designing and implementing INSM could result in endless arguments among Responsible Entities, Regions, and NERC over what might be considered acceptable risk-based approaches. We are even more concerned about the proposed criteria for Severe VSL for R1 ("The Responsible Entity did not identify network data collection locations and methods that provide value,..."). What is "provide value" intended to mean, and who would have the final say on whether a given Entity's INSM implementation was capable of doing so? NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection locations and methods used to monitor network activity including connections, devices, and network communications."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT received feedback that a provision is needed to allow for risk-based options. The Technical Rationale provides additional insights for Requirement R1, Part 1.1.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to IRC SRC's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that the Standard does not address scenarios in which no technical solution is available to achieve what the Standard requires, such as when an entity's environment includes devices that use non-standard	

communication protocols. The SRC recommends that the standard be revised to address these types of scenarios, such as by allowing entities to apply for a Technical Feasibility Exception if circumstances warrant.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. The Technical Rationale provides additional insights for Requirement R1, Part 1.1. Furthermore, it is the DT's opinion that a well-developed, risk-based rationale would avoid the need to file and maintain a Technical Feasibility Exception.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE is not in agreement with EEI's comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT is unable to address your concern(s) since it is not indicated specifically what you disagree.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No

Document Name	
Comment	
AZPS agrees with EEI proposed revision to CIP-015-1 R1, Part 1.1: "Identify network data collection location(s) **point(s)** and method(s), based on the network security **threat(s)** risk(s) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern agrees with and greatly appreciates the discussion in the TR on Part 1.1 and the degree of flexibility described there to "narrow the focus to collect the data that provides the highest benefit" and "narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data". However, Southern suggests that R1 as worded implies a scope of 100% coverage of every subnet within in-scope ESPs. It is not until an example under the R1.1 measures that it mentions the potential exclusion of any network locations and the documentation of such. The TR states many different aspects to consider in choosing monitoring locations (value, benefit, cost-effectiveness, relevance, etc.) but R1.1 limits it to only network security risks. There is concern with the implication of "do all, but explain where you don't" that this could require the documentation of network security risks for each IP subnet and "prove the negative" type evidence. As page 4 of the TR states network data collection location refers to both physical and logical networks, so there is concern with the large proliferation of logical networks with containerization (what used to be API calls are being replaced with virtual networks and IP addresses assigned to containers). Zero Trust principles and containerization call for ever more micro-segmentation and creation of virtual networks down to this level between	

components of an application in a single system. As an example, documented reasons of why an entity did not monitor every internal virtual network generated by Docker between two components of a single application within a single Cyber Asset one could argue are of little value, but it seems would be necessary.

For all these reasons, we suggest a concept of a positive "identify where you do" rather than a sense of "explaining and documenting where you don't". The value of where to monitor is going to be based on the system's architecture, especially in large, multi-layered, distributed systems. On the other end of the spectrum is a site that may have a router with an ACL on an ethernet port to an RTU, which is then connected serially to several relays. Monitoring that 2 node, single ethernet cable "internal network" ESP may be of no value as all traffic can be monitored on the other end of the circuit, and it is unclear whether the entity is compliant if they do so.

Southern suggests a concept for R1 and 1.1 such as:

R1. Responsible Entity shall implement one or more documented process(es) for Internal Network Security Monitoring (INSM) that includes:

R1.1 Identification of network data collection points by the Responsible Entity for its high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC).

We suggest that this covers monitoring the in-scope systems, but leaves flexibility on where such monitoring occurs on its networks and doesn't imply "prove the negative" for every physical/virtual subnet that is not tapped and monitored.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language.

Robert Follini - Avista - Avista Corporation - 3

Answer	No

Document Name	
Comment	

Avista agrees with comments by EEI (words in italics are requested to be struck)

EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

"Identify network data collection *location(s)* **point(s)** and *method(s)*, based on the network security **threat(s)** *risk(s)* **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	

"***R1.1*** *Identify network data collection locations and methods,* ***based on the network security risk(s)****, to monitor network activity including connections, devices, and network communications*."

The bolded part ("based on the network security risk(s)") is not clear and can be open to interpretation of what is required. Therefore, it is recommended to require identification of the specific data collection locations and methods based on an entity's own experience and system needs.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The "risk-based" language leaves it open for auditor interpretation. Meaning, auditors can determine that an entity did not apply the appropriate "risk-based" approach for their network security. BPA believes some level of deference must be offered to an entity's risk management approach. Or, create auditor guidance on what a risk-based approach looks like with regards to INSM.

BPA reiterates its comments from the previous comment period regarding 'risk-based approach':

"BPA recognizes and appreciates the SDT's effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors... BPA suggests that R1.1 be rewritten to more clearly specify the requirement, such as "Use a risk-based assessment methodology to identify network data collection locations and methods…" Language used elsewhere in the CIP Standards, such as "as determined by the Registered Entity", could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc." BPA also asks the DT to clarify the term "locations" in the requirement, adding context currently only found in the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. In addition, the DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)".	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The current R1.1 requirements could be interpreted that a "Network Security Risk" evaluation or assessment could be required under the standard. Cogentrix suggests removing "Network Security Risk" or stating that INSM should be for monitoring of the entire network per technical capability or assets "Network Security Risk" for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated clearly in the standard. Furthermore, greater specificity should be offered for what 'network activity' entails. For connections,	

monitored activity should include who, when, why, and how long; network communications should include type, port, bi-direction or unilateral, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities. The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider ***all*** possible network data collection locations. For example, and entity may decide to "collect all traffic from INSM from all ESP switches", which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as "Documented rationale on how network locations were selected or excluded", and the Technical Rationale "requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes."	

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify "collection of traffic from all network switches", then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language: "Identify network data collection (*remove*: location(s)) **point(s)** (*remove*: and method(s)), based on the network security **threat(s)** (*remove*: risk(s)) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications."	

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM. We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based	

rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy recommends the use of the word “points” instead of “locations” in R1.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Moreover, the DT received comments that reference “locations” could be confused with geographic locations, and the DT modified “network data locations and methods” with “network data feed(s)”.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES Support EEI comment below	

EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: “Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications.” EEI proposes modifications to the draft M1, Part 1.1 measures to: “Architecture documents or other documents detailing data collection location(s) and method(s); or”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI’s comments.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
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 Collaborators	
Answer	Yes
Document Name	
Comment	

While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains "and allow for future expansion if necessary", makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
While Requirement R1, Part 1.1 is clear in intent, it must be supported by guidance on acceptable methods of monitoring network activity. For example, is monitoring activity at endpoints acceptable, or is dedicated monitoring equipment required? If a zero-trust strategy is implemented, can monitoring attempts to establish connections outside of the zero-trust architecture satisfy this requirement, or is a more traditional network intrusion detection solution required? It may not be practical to address such questions in the standard, but guidance documents that include technology options must reflect and support the intentions of the SDT.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. While end-point monitoring can be useful for an INSM program, the goal of the proposed Reliability Standard CIP-015-1 is monitoring network data feeds within the trusted zone.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Georgia System Operations Corporation supports ACES comments: "While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains 'and allow for future expansion if necessary', makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
SPP respectfully asks the SDT to consider a "per system capability" clause due to potential technology limitations for entities (current and future technologies).	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
SMECO agrees with ACES comments: While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains "and allow for future expansion if necessary", makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	

Comment	
CIP-015 R1.1 goes beyond the requirements in CIP-007. If we are logging events at a BES system level per the Cyber Asset capability then the network locations are already identified at the layer 2 and layer 3 devices within the scope of the existing cybersecurity monitoring program. By not updating existing monitoring standards the new standards are introducing additional complications to demonstrating how the monitoring program works overall. The statement based on network security risk(s) is vague on what risk should be evaluated or included in the assessment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. While end-point monitoring can be useful for an INSM program, the goal of proposed Reliability Standard CIP-015-1 is monitoring network data feeds within the trusted zone.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. TFIST suggest removing “Network Security Risk” or stating that INSM should be for monitored of the entire network per technical capability or assets “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based	

rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned the enforceable language of the requirement does not specify that the Responsible Entity is required to document the rational/justification for inclusion or exclusion of data collection location(s) and method(s) based on a risk-based approach in determining what data is necessary to monitor network activity. The SDT should consider requiring entities to justify the parameters they have developed to meet the requirement. The SAR for this project states, “Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communications, and software inside the CIP-networked environment.” Texas RE noticed that software inside the CIP-networked environment is omitted from the requirement language. If the SDT intentionally omitted this language, then no change is needed. If the SDT did not intend to omit the language, Texas RE recommends including software in the requirement language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this	

Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale. Moreover, the DT reviewed the SAR, and with respect to the reference to monitor network activity including software, the opinion of the DT is the network data related to software will be included in the elements contained in Requirement R1, Part 1.1.	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities. The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider ***all*** possible network data collection locations. For example, and entity may decide to "collect all traffic from INSM from all ESP switches", which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as "Documented rationale on how network locations were selected or excluded", and the Technical Rationale "requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes." If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify "collection of traffic from all network switches", then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

5. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AEs Supports EEI comment below EEI appreciates the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.” As described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with EEI comments below: "The description of of the term "baseline" in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that "[m]any vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not." "As described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	

If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL[1]

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

[1] https://www.merriam-webster.com/dictionary/anomalous

1.4. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.5. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.6. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	

Comment

If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL[2]

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version. However, It is clear that detection of anomalous activity has to be referenced to some standard/metric so it would appear that a baseline would be required, and as such should be stated explicitly.

Further, this approach appears inconsistent with existing requirements in CIP-007, R4, which calls for generation of alerts for security events. Should not this capability exist for ISNM as well that could then be evaluated in R1.3?

[2] https://www.merriam-webster.com/dictionary/anomalous

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

While CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT believes that most entities are logging events at the Cyber Asset level in a security information and event management (SIEM) system. Additionally, the SIEM may be used for analysis and retention of those host-level events to meet CIP-007-6, Requirement R4 and allow for detection of login attempts and malicious code on those Cyber Assets.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST disagrees with the SDT's decision to demote network baselining from a Requirement to a Measure, which is essentially nothing more than a suggestion, for two reasons:

> FERC Order 887 Paragraph 5 states explicitly, "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment."

> We are hard-pressed to imagine how anyone using INSM could detect anomalous network behavior without a baseline. To that point, Order 887 Paragraph 12 states, "Establishing baseline network traffic allows entities to define what is and is not normal and expected network activity and determine whether observed anomalous activity warrants further investigation."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not. Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2. The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	No
Document Name	
Comment	
Tacoma Power supports the EEI comments for consistency of language on what to detect (i.e. anomalous or unauthorized). Tacoma Power thinks the language change to Part 1.2 is non-substantive and could be made for the final ballot posting.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to NPCC RSC's comments.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	No
Document Name	
Comment	
Part 1.2 refers to "data collected at locations identified in Part 1.1," but it seems that depending on the method used to collect and identify anomalous information, the data collection location may not be relevant. Suggested language: "Implement one or more method(s) to detect anomalous network activity using the data collected pursuant to Part 1.1."	
Likes 0	

Dislikes 0	

Response

Thank you for your comment. The DT updated Requirement R1, Parts 1.1., 1.2., and 1.3 for clarity.

1.4. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.5. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.6. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

This would require knowledge of previous context and in order to be compliant, it appears that a baseline would be required to compare network activity to detect “anomalous” activity. SRP strongly feels that it should be stated specifically in the standard. Also, as previously stated, the requirement is still not clear of the word "baseline" and perhaps a definition or explanation should be included in the measurements section. SRP also suggest that in the Methods it includes what the Technical rational has defined as a "baseline" as the word "baseline" is still confusing since the baseline is also used in CIP-010 R1.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2. The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.	
Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	
Seminole supports the comments from EEI "The description of the term "baseline" in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that "[m]any vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees that Part 1.2 is clear and an objective-based approach that requires one of more methods to detect anomalous network activity without the prescriptive requirement of a baseline.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation agrees with EEI's comments: EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term "baseline" in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that "[m]any vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes

Document Name	
Comment	
MRO NSRF appreciates and endorses this approach, which is clear in its intent. However, there is a concern that the phrase “detecting anomalous or unauthorized network activity” in R1 does not align well with Parts 1.2 and 1.3. We recommend striking “or unauthorized” in R1 to better align with the rest of the standard. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT agrees that striking “or unauthorized” in Requirement R1 better aligns with the other requirements in the proposed standard and updated Requirement R1 for Draft 2.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA endorses removing "baseline" language from the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the feedback by EEI. In addition, we do note the wording in the 1.2 requirement part is “anomalous”, but the measure switches to “unauthorized”. Per our comment on R1, we would suggest this be changed in the measure to match the requirement. A baseline of normal traffic could be used to show what is anomalous but would not determine what is unauthorized.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments. The DT updated the Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	

Comment	
Including measures referencing documentation of a network baseline not included in the standard does not make it an obligation of the requirement. Suggest remove from the measures. Instead, suggest the standard list specific events that an entity should be looking for as a minimum requirement.	
Likes 0	
Dislikes 0	

Response
Thank you for your support. The DT updated the Requirements, Requirement Parts, and Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not. Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2. The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

PNMR agrees with the SDT to remove the term “baseline” from the requirement language. It does, however, believe that the term “baseline” in the Technical Rationale should be replaced with “expected network behavior”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT updated the Technical Rationale document to include a parenthetical after the word “baseline” “(expected network behavior).”	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support’s EEI’s comment(s): EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
David Jendras Sr - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	

Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
M1 1.2 -The phrase "Documentation of baseline used" does not adequately capture how these tools work. Some entities configure settings of these tools to only alert on exceptions to a baseline, but it's not like the software baseline that is easily discernable. Explicit baselines may be problematic since the tools are typically based on learning to detect anomalies, though feels our approach would be to provide the configuration settings used for the monitoring tool. This is more of a conpliance concern as some entities may leverage other options to demonstrate compliance than a baseline.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT updated Measure 1, Part 1.2 for Draft 2 of proposed Reliability Standard CIP-015-1: • Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes 0	
Dislikes 0	

Response

Thank you for your support.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

Likes 0	
Dislikes 0	

Response

Thank you for your support.

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned with the removal of explicit requirements such as baselining to accomplish the security objective of implementing methods to detect anomalous network traffic. FERC Order No. 887 recognizes that establishing baselines is the primary means to identify anomalous traffic within an entities' CIP-network environment, noting that "any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment." FERC Order No. 887, at ¶ 79. Texas RE notes that FERC Order No. 887 does contemplate that the final rule should "provide flexibility to responsible entities in determining the best way to identify anomalous activity to a high-level of confidence, so long as the methods ensure: (1) logging of network traffic . . . (2) maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation, and (3) maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures . . .. FERC Order No. 887, at ¶ 80.

While recognizing this need for flexibility, however, Texas RE is concerned that some of the identified measures, such as a list of detection events or INSM configuration settings, may be too vague to provide meaningful evidence that the detection of anomalous network activity security objective is being meaningfully performed. To prevent this, Texas RE suggests inserting language in the measures that clarify that, at a minimum, data collection methods must be of sufficient data fidelity to draw meaningful conclusions and support incident investigation consistent with the language in FERC Order No. 887.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT updated the Requirements, Requirement Parts, and Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1.

Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not. Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2. The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	

Comment
The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards is ambiguous on if a baseline is required in its current version.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not. Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

A clear definition of “anomalous” is needed in order to determine compliance. For example, in Generation, certain activity that may take place during an outage may not be considered “anomalous” and would not invoke CIP-008. Also, the wording "Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action." is of a concern. It is vague and lets entities make their own decisions, which could be seen as audit bait when being audited.

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL[3]

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.7. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.8. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.9. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

BC Hydro has concerns in relation to the use of term "anomalous activity" as this could be varied in terms of application and usage and is left to the entities to interpret.

BC Hydro also has concerns over the expected evidence needed for "documentation of responses to detected anomalies" per Measure M1 to meet Part R1.3., which seems to indicate that proof that all detections were responded to regardless whether they were false positives will be required, i.e. proving the negative on all anomalies detected. Due to this BC Hydro has concerns over a very high amount of data which needs to be analyzed and documented based on Requirement R1 Part R1.3 as drafted.

[3] https://www.merriam-webster.com/dictionary/anomalous

BC Hydro recommends to make the scope concise in the language of CIP-015 Requirement R1 Part R1.3, and add example scenarios and use-cases in the Technical Rationale.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT felt "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL[4]

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.10. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.11. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.12. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

[4] https://www.merriam-webster.com/dictionary/anomalous

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA agrees with EEI comments about the word "appropriate" being too open for interpretation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with EEI comments below: "The term "appropriate" is a subjective term. We propose the following revision: "Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2" This language is similar to the language used in CIP-008-6. Additionally, as described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see responses to EEI's comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy believes that the "appropriate action" language is too subjective and should be removed. We understand that in the process of tuning INSM implementations may generate lots of alerts, with the majority being false positives. We think that there is a way to tie the language to CIP-008 without arbitrarily treating each alert as an attempt to compromise. We suggest "Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine if a CIP-008 Cyber Security Incident response plan activation is required as a response.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT removed "appropriate action" and replaced it with "further action(s)". Requirement 1, Part 1.3. was updated for Draft 2 to, "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES agrees that Part R1.3 provides entities the flexibility to evaluate and determine appropriate action. However, from the point where a determination is made and going forward, all related activities should be driven by existing Requirements in CIP-008.	

AES also agrees with EEI comment below

EEI appreciates the SDT's revisions to allow Registered Entities to have flexibility to evaluate activity detected in Part 1.2 to determine appropriate action, however, the term "appropriate" is a subjective term. We propose the following revision: "Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2" This language is similar to the language used in CIP-008-6.

Additionally, as described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses to EEI's comments. Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after the evaluation in Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's CIP-008 incident response process(es) for further investigation.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	

Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Since Part 1.3 requires two separate actions, SPP recommends the following edit to the proposed language in R1, Part 1.3 (I.e., "change the word "to" to "and"): Implement one or more method(s) to evaluate activity detected in Part 1.2 and determine appropriate action.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT disagreed with your suggestion to change "to" to "and," but did revise Requirement R1, Part 1.3: **1.3.** Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
The way the measures for Part 1.3 are written, it appears entities could select just one. Was this the intent of the DT? Consider revising to clarify that documentation is needed for evaluating and responding to anomalous or unauthorized network activity and an escalation process linking it to CIP-008.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Network and metadata associated with anomalous network activity must be available for the evaluation conducted in CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after evaluated in Requirement R1, Part 1.3. However, data associated with potential	

attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's CIP-008 incident response process(es) for further investigation.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Section C of the standard provides information on evidence retention.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment
No additional comments

Likes 0	
Dislikes 0	

Response
Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
BPA believes there is still room for clarification to revise “anomalous network activity” to “anomalous conditions”. Network conditions can include lack of activity or states.

Likes 0	
Dislikes 0	

Response
Thank you for your support. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary. Anomalous - adjective 1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	

Comment	
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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 6.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
While the measures do provide guidance, the requirement language should be clear in the intent. Texas RE recommends the following language to clarify the intent of Requirement Part 1.3: R1.3 Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action, up to and including identifying the anomalous network activity as a Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT updated **Requirement 1,** "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts:" In addition, the DT updated **Requirement R1, Part 1.3,** "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."	

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES agrees with protecting INSM data from being inadvertently deleted or modified. However, we do not want the categorization or treatment of INSM data be conflated with or mistaken for BCSI. The two types of information must be treated as two separate and discrete types of information.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT agrees that the data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[5]" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	

[5] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Answer	No
Document Name	
Comment	
Duke Energy sees additional opportunities for clarification in R2. We are concerned that R2 is redundant for entities who will classify their INSM systems as EACMs, and that the flexibility in INSM system classification is not clear. We propose “Responsible Entity with an INSM system not classified as an EACM shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT agrees there may be some overlap in requirements. The intention of specifying the requirement under R2 ensures the protection is in place regardless of the categorization of the INSM system.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Black Hills Corporation seeks clarification on \how this Requirement R2 differs from the existing CIP-011 language regarding data protection, as we would like to see a standard that does not duplicate or conflict with existing CIP requirement language. Black Hills Corporation also agrees with the comments from EEI: EEI proposes the following revision to CIP-015-1 R2: Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (*remove*: , except during CIP Exceptional Circumstances).	

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement. EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing " should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI's comments.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. The standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data. Furthermore, Cogentrix proposes that ISNM data be specifically added as an item for CIP-011 classification as BCSI; as a result, this requirement is not needed.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT agrees that the data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[6]" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
The way in which this requirement reads there are CIP-012 overtones. Protecting data against the risks of 'unauthorized deletion or modification' is too close to the goal/objective of CIP-012, creating confusion and cross-over.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has also updated the Technical Rationale document for clarity on Requirement R2. Additionally, the DT has also created a FAQ document for this project that states, "Because network traffic captured in transit between hosts cannot typically be	

[6] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network."	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agree with EEI comments EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE support's EEI's comment(s): EEI proposes the following revision to CIP-015-1 R2: Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement. EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #7.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.” Additionally, the DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI’s comments.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, there are a variety of of events, logs and other evidence based output that is generated by other CIP standards that don't require this level of protection. This appears to be overreaching in the protection of data that is beyond the protection of the BCS requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has also created a FAQ document for this project that states, "Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network."	

Additionally, the DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
It is not clear if the Requirement R2 is expecting both detection of unauthorized access and/or changes along with protection mechanisms to prevent unauthorized access or if the entity can choose what combination of controls is appropriate to them based on their security risk tolerance. BC Hydro recommends to provide clarity in the Requirement R2 to remove ambiguity and scope these accurately. BC Hydro also notes that although Technical Rationale provides examples of guidance it is not an ERO endorsed compliance guidance document. Auditors may chose to adhere to certain aspects from Technical Rationale and choose to leave others.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Requirement R2 has been revised to: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification."	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	

Comment
EEI proposes the following revision to CIP-015-1 R2: Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement. EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see responses to EEI’s comments.

Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	

Comment
See comments submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. NPCC RSC is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data."	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Please see responses to NPCC RSC's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Does this suggest that the RE maintain the evidence? Why? For how long? What is the purpose and intent of this requirement? Could CIP-004 (access), CIP-005 (vendor access) or CIP-011 (BCSI protections) be leveraged for this purpose? Clarification is needes as it is not clear what the purpose and intent of this requirement is. What does "To mitigate the risk of unauthorized deletion or modification" mean? Again, shouldn't CIP-004 R4 and CIP-011 address this? Also, do the individuals who have the access, be the ones authorized to have the access. One concern is when vendors who have this access, and how would an entity monitor for such activity?	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.” The Technical Rationale has been updated to provide further clarity.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI proposes the following revision to CIP-015-1 R2: "Responsible Entity shall implement***, except during CIP Exceptional Circumstances,*** one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification." As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement. EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.” The Technical Rationale has been updated to provide further clarity.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale: BHE seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. BHE seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Data protection in CIP-015-1, Requirement R2, is intended to protect the data from being altered or removed by an advisory intended to cover their tracks. BCSI protection as defined in the CMEP guide and CIP-011 is to protect against data or information that could be used to gain unauthorized access to a BES Cyber System.	
Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	

Seminole agrees the EEI

EEI Response:

Responsible Entity shall implement**, except during CIP Exceptional Circumstances,** one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes there is an operational concern that logs should be set to over-write rather than causing a full disk stop condition. This may be a higher priority than keeping all logs, as the proliferation of security event logs, in itself, is an indicator of an issue that can feed into response activities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT has revised Measure M2: Evidence may include, but is not limited to, documentation demonstrating how data is being protected from the risk of unauthorized deletion or modification.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
The protection of the data does not need additional standards since a risk has not been identified that this newly created data element is subject to. Why would this data be subject to risk of unauthorized deletion or modification compared to other security logs or data?	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Project 2023-03 INSM is addressing FERC Order No. 887.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF recommends placing the following statement “except during CIP Exceptional Circumstances” after the word implement which specifies the action for the phrase rather than a general statement.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. The updated requirement reads: Requirement R2: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.”	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale:	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. TFIST is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. The DT has revised Requirement R2 to: "Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification." The DT has also updated the Technical Rationale document for clarity on Requirement R2.

Additionally, the DT has also created a FAQ document for this project that states, "Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network."

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. – 6	
Answer	No
Document Name	
Comment	

Seminole Agrees with the comments from MRO NSRF

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses to MRO NSRF's comments.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
Document Name	2023-03_Comment_Form_MRO_NSRF_20240313_Final.docx

Comment

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network

communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests **eliminating CIP-015 R3** and **adding a new sub part 1.4** a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT made the following changes that we believe will hopefully address the concerns listed.

- The DT added a note to R3 stating:

  "Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."

- The DT is hesitant to have potential overlap with an entity's existing CIP-008 processes. We altered Part 1.3 to state:

  "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s)."

  The implication is that anomalous activity will require a response that could range from tuning software if the activity is noise to escalating into the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.

Jennifer Neville - Western Area Power Administration – 6

Answer	No
Document Name	

Comment

Concerns with the language in R3. The amount of data to be collected and stored is extremely voluminous, which in turn is a very expensive administrative burden that does not provide additional security or reliability. Suggest modifying the language for R1.2 and R1.3 to reflect limiting the data retained to network communications and other related data as part of the investigated alert.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed. • A note has been added to R3 stating: "Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp – 6	
Answer	No
Document Name	
Comment	
BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows: "Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail for at least ninety days,** INSM data **evaluated** in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances." The choice for "ninety days" duration is meant to keep consistency with other CIP Standard log retention requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed. A note has been added to R3 stating:	

"Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows: "Responsible Entity shall implement one or more documented process(es) to retain***, with sufficient detail and duration, INSM data evaluated in support of*** Requirement 1, Part 1.3 ***and determined by the Responsible Entity to be anomalous and require action***, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed. • Requirement R3 was revised to the following: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
The phrase "retain network communications data AND other metadata." This insinuates that entities may need full PCAP monitoring of an entire BCS and retaining entire conversations. This could require significant allocation of resources from entities, especially if storage is required for a significant amount of time. Entities should be able to establish retention requirements in their program for full PCAP if required to implement as this approach may not be cost effective for entities.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed. Requirement R3 was revised to the following: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

It is unclear as to how to meet any objectives of this requirement. Again, the word anomalous needs clarification. The way the requirement is written is still vague in determining how long to retain network communications data and meta data collected with sufficient detail and duration to support the analysis. The technical guidelines has more in-depth information on what should and can be the length of time. However, as we all know, auditors will be auditing to the Standard and requirements and not the technical rational. Maybe include additional information in the measures section?

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.

Requirement R3 was revised to the following:

"Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2."

The DT considered whether or not to create a NERC Glossary term for "anomalous." After reviewing the Merriam-Webster dictionary definition, the DT felt "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	
Comment	
ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	No
Document Name	
Comment	
The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. The data to be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other	

related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System. *Consider:* *R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Georgia System Operations Corporation supports ACES comments: "ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments:	

"R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. NPCC RSC is unclear on what “sufficient detail and duration” means and if these words are necessary."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to NPCC RSC’s comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI’s comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI’s comments.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks that the SDT provide additional clarity around (i) what is a reasonable duration for network communications data and metadata retention, and what is defined as network communications data and metadat	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
It is unclear on how long the data needs to be retained. Suggest including a clear timeline minimum 90 days to match with CIP-007 R4.3 event Log retention	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following:	

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:	

"Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro has concerns about the extensive data volume and high costs associated with Requirement R3 per the current language. BC Hydro suggests limiting retained data to network communications and relevant information linked to investigated alerts only. A full capture of network data poses excessive burdens in terms of cost and sustainment and does not contribute extensively in enhancing security or reliability for the Bulk Electric System. BC Hydro recommends that the DT narrow the scope of INSM (Internal Network Security Monitoring) data to only Attempt to Compromises and reportable Cyber Security Incidents only in line with CIP-008 requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following:	

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows: "Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail for at least ninety days,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances." The choice for "ninety days" duration is meant to keep consistency with other CIP Standard log retention requirements.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	

No, NCPA agrees with AES statement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to AES's comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPC has signed on to ACES comments:	

ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes R3 should clarify it is left to Registered Entities to decide what collected data should be retained and for how long. We suggest, "Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration, *as determined by the Responsible Entity,* to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following:	

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to IRC SRC's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see responses to EEI's comments.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The SRC recommends that the standard be revised to provide additional clarity regarding the extent of a Responsible Entity's ability to define and determine what data (particularly metadata) needs to be retained and the appropriate retention period. Without additional clarity, the	

SRC is concerned that Requirement R3 could be construed to require entities to retain large amounts of data for the full duration of the three-year evidence retention period applicable to CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE support's EEI's comment(s): EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:	

"Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
AZPS agrees with EEI's concerns regarding the proposed language for CIP-015-1 R3. Potential ambiguity in the current draft of data collection requirements may lead to interpretations which require significant data collection and storage. AZPS supports the following revised language: "Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	No
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI's comment -- EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	

Comment
"***R3*** *Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected* ***with sufficient detail and duration*** *to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances*." The bolded part ("with sufficient detail and duration") is unquantifiable and can potentially be too subjective. LDWP would recommend specific criteria or additional technical guidance be included for what "sufficient detail and duration" entails.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO NSRF's comments.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. This brings the question of what "sufficient detail and duration" means and are these words are necessary? Further, other approved CIP standards offer specific data retention periods. Cogentrix does not believe this ambiguity is helpful to the objective and the DT should specify a timeframe to help clarify entity expectations and introduce consistency in application.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following:	

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
Black Hills Corporation agrees with EEI's comments: EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows: "Responsible Entity shall implement one or more documented process(es) to retain**, with sufficient detail and duration,** (*remove:* network communications data and other meta data) INSM data (*remove*: collected with sufficient detail and duration) **evaluated** (*remove:* to support the analysis) in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI's comments.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	

Comment
The proposed language in R1 1.3 and R3 is ambiguous and should be revised. Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.

Likes 0	
Dislikes 0	

Response
Thank you for your comment.

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment
Tri-State agrees with the comments below: AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System. To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

*1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.*

*1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred.***

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

***1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall* initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.**

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see response to AES.
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	
Comment	
Duke Energy suggests additional clarification on the retention expectation for R3 and removal of the language “sufficient detail and duration”. We would suggest this alternative language “Responsible Entity shall implement one or more documented process(es) to retain network communications data collected to complete the analysis in Requirement R1, Part 1.3 and to execute their Cyber Security Incident response plan where required.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Is there an intended difference between “INSM data collected” as referenced in R2 when compared to “network communications data and other meta data collected” as referenced in R3? If this is the same thing, ATC supports the intent of the requirement, but requests consideration of using consistent terminology for clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The current revision of R2 addresses the concerns that you listed above: R2. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12.

This will likely be more of a function of cost versus want. Depending on number of alerts and need to keep for entire audit period.

Likes 0	
Dislikes 0	

Response

Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	Yes
Document Name	

Comment

LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12.

Likes 0	
Dislikes 0	

Response

Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer	Yes
Document Name	

Comment

PNMR agrees with R3, but to more closely align with R2, which states entities must protect INSM Data, PNMR believes the language of R3 should read:

“Responsible Entity shall implement one or more documented process(es) to retain internal network security monitoring data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.”

Likes 0	
Dislikes 0	

Response

Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]	

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA recommends that a suggested minimum retention parameter be included in the Technical Rationale. BPA believes this would be in alignment with language cited in CIP-007 R4, 90-day event log retentions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed.	

Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. TFIST is unclear on what “sufficient detail and duration” mean and if these words are necessary.	
Likes 0	

Dislikes 0	

Response

Thank you for your comment. The DT has made the following change that we believe will hopefully address the comment listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is concerned that not establishing guidelines or thresholds for minimum retention periods, this requirement would be a challenge to comply with, audit, and enforce consistently. Texas RE notes that FERC Order No. 887 specifically identifies the need to "maintain . . . logs, and other data collected, regarding network traffic" as key security objective for the implementation of an effective INSM program. Failure to maintain evidence of the collection of log data renders this security objective essentially unenforceable.

Texas RE concedes that a blanket requirement to retain logs may not be appropriate to meet this security objective. For example, from a storage perspective it would be very expensive to require network traffic of full system backups to be stored for 90 days. Likewise, from a threat perspective this is known and expected traffic and would be of minimal benefit to store. As such, Texas RE recommends adding language to the requirement for Registered Entities to explicitly define types of traffic that will not be required to be retained. Registered Entities could write into their program that expected traffic will be excluded from storage and retention requirements. However, this

expectation should be clear from the requirement language itself, and the burden placed on entities to carefully define and demonstrate they are accomplishing the FERC-mandated security objective to retain maintain sufficient logs regarding network traffic so that can detect anomalous events and effectively demonstrate compliance with that expectation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed. Requirement R3 has been revised to the following: Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	
Document Name	
Comment	
AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive.	

AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

*1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.*

*1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred.***

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

***1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall* initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.**

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Option 2:

If the DT does not agree with Option 1, AES suggests modifying R3 to read:

R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration ***collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3****, except during CIP Exceptional Circumstances.*

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following changes that we believe will hopefully address the concerns listed.

- Requirement R3 has been revised to the following:

  Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

- Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.
- The DT is hesitant to have potential overlap with an entity's existing CIP-008 processes. We have altered Part 1.3 to state:

  "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s)."

  The implication is that anomalous activity will require a response that could range from tuning software if the activity is noise to escalating to the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
AES agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
No, Southern Indiana Gas & Electric (SIGE) does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in	

order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
No, CenterPoint Energy Houston Electric (CEHE) does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. CEHE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.. The undertaking will demand significant effort, substantial capital investment and additional staffing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA reiterates its comments from the previous comment period regarding the proposed implementation plan timeline.

BPA's previous comments: "After reviewing the new requirement language in CIP-015-1, BPA believes more time will be required to implement an INSM program. This takes into consideration the initial effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'"

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees with the feedback by EEI.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
This Standard's implementation as drafted can be very time and cost intensive due to language in R3 as commented in response to Question #8 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement. Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No

Document Name	
Comment	
SRP would need for the questions above to be answered and the standard to be clearer before we can make a determination on a timeline. Currently the standard is written as a Subjective standard vs. an Objective standard and additional clarity would be needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 Implementation Plan timing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation agrees with EEI comments: EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
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 comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

MRO NSRF agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment	
NEE support's EEI's comment(s): EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "NPCC RSC agrees with the implementation plan."	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to NPCC SRC's comments.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Georgia System Operations Corporation supports ACES comments: "While ACES does not oppose a 36 month implementation plan, ACES believes the INSM OT industry and ERO lack sufficient SMEs to get this implemented fully by all entities across the ERO in 36 months. ACES feels there needs to be an extension provision in the implementation plan."	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to ACES' comments.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Constellation feels strongly that more than 18 calendar months is needed for implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of	

vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC defers to the comments by the applicable entites on the Implementation Plan	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	

Was not discussed on 3/7/2024 meeting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
More clarity within the requirements is needed to determine cost-effectiveness of needed controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has made revisions to proposed Reliability Standard CIP-015-1 based on industry comments.	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
This standard will require substantial investments in infrastructure to accomplish the monitoring objects, as well as additional personnel to provide adequate monitoring coverage and support of these systems and associated compliance requirements. A more flexible standard that incorporates monitoring from the endpoint would align more closely with existing security monitoring initiatives. Cost-effectiveness is not possible to determine with the limited clarifications at this time. More information is needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds,	

cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

Georgia System Operations Corporation supports ACES comments:

"ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

The risk needing to be reduced or closed
How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective

How much vendors will increase prices due to INSM requirements Implementation capital cost Annual Operation and Maintenance cost How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan Market analysis of SMEs needed to manage INSM as required"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks the SDT to consider the potential cost that may arise from the scope of these requirements. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, managing, and storing of all INSM data and metadata for any length of time will be substantial	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability	

Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement. Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Please refer to comments in Question #8 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to Question 8.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA would need further analysis to detertime the cost effecivness of the proposed standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPC has signed on to ACES comments: ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the	

most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

1. The risk needing to be reduced or closed
2. How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective
3. How much vendors will increase prices due to INSM requirements
4. Implementation capital cost
5. Annual Operation and Maintenance cost
6. How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan
7. Market analysis of SMEs needed to manage INSM as required

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see responses to ACES' comments.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to IRC SRC's comments.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds,	

cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The SRC is concerned that the issues identified in its responses to questions 4 and 8 could materially impact the cost of meeting the underlying reliability goal and FERC directives. Specifically, if Requirement R1 is not clarified as discussed in the SRC's response to question 4, Responsible Entities may have to incur costs to upgrade or replace equipment that uses nonstandard communication protocols for which no effective INSM technology exists. If Requirement R3 is not clarified as discussed in the SRC's response to question 8, Responsible Entities may need to incur the costs of storing large quantities of data for the duration of the three-year CIP-015-1 evidence retention period.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT made revisions in the requirements based on industry's comments.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No

Document Name	
Comment	
Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications 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. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Without further study the costs associated cannot be determined at this time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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	
PG&E does not have any current way to judge the cost-effectiveness of these requirements until the modifications have been approved.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
No, without further study, CEHE believes the costs associated with the new requirements cannot be determined. Some substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment
No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.

Likes 0	
Dislikes 0	

Response
Thank you for your comment.

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	

Comment
NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.

Likes 0	
Dislikes 0	

Response
Thank you for your comment.

Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support and comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
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	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
Was not discussed on 3/7/2024 meeting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC defers to the comments by the applicable entites on the Cost Effectiveness of the Standard.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	
Document Name	
Comment	
NST lacks the information necessary to comment on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	

NEE does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA reiterates its comments from the previous comment period regarding cost-effectiveness. BPA's previous comments: BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	

MRO NSRF has no comment on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	
Comment	
No. From a generation facility perspective, this would be a heavy lift and substantial cost burden. As indiciated on the INSM survey submitted last year, owners with multiple assets (especially generaiton) do not have baked-in cost recovery mechanisms. LS Power Development recommends referring to survey responses, specifically those from GO/GOPs. IT/OT support services at the plant level is a relatively newer initiative, and network infrastructure requirements per CIP-015 (though practical and good cyber security practice) are still cripling cost-wise. Other than performing a study to realize the actual risks to generation facilities, there presently isn't sufficient justificaiton.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Project 2023-03 INSM was created in response to FERC Order No. 887. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	

Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	
Document Name	
Comment	
Will need to research a solution to see if it is cost effective.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	
Will need to research a solution to see if it is cost effective.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

11. Please provide any additional comments for the DT to consider, if desired.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, 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 DT for their consideration of the industry's input which included the creation of CIP-015 and the modifications from the last ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation recommends adding the following definition to the NERC Glossary of Terms: Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences. Reclamation appreciates the DT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the DT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary. Anomalous - adjective 1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL Example - Researchers could not explain the anomalous test results. 2 a: of uncertain nature or classification b: marked by incongruity or contradiction : PARADOXICAL
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	
Document Name	
Comment	
Black Hills Corporation repeats EEI’s comments: EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI’s comments. Generator Owners have been included in Section 4 Applicability. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment	
Cogentrix recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to MRO NSRF's comments.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	
Document Name	
Comment	

Thank you so much for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
Generator Owner was left out of applicability, should be re-added.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Generator Owners have been included in Section 4 Applicability.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
While TVA appreciates the flexibility afforded by the proposed risk-based language, additional clarity or assurance regarding how the CEA will approach auditing and determine sufficiency would be helpful.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE support's EEI's comment(s): EI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	

Response
Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).
David Jendras Sr - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment
Ameren agrees with and supports EEI comments.

Likes 0	
Dislikes 0	

Response
Thank you for your comment. Please see responses to EEI's comments.
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment
NST respectfully offers the following comments/suggestions on the Technical Rationale document: > The document includes several statements about compliance that seem to have been written as statements of fact. Three examples, numbered for reference purposes, are: (1) "Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R1, Part 1.2 or 1.3."

(2) "Short periods of reduced visibility should not justify a potential non-compliance finding, especially when other cybersecurity monitoring is in place."

(3)"Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2."

NST believes it is beyond the SDT's purview to make such assertions, and we therefore recommend they be reworded to clarify they only represent STD opinions.

With regard to statement (1) and the idea of suspending INMS monitoring or suppressing alerts while maintenance and/or system upgrade activities are in progress, we believe a better approach to allowing an Entity to do this without risking instances of non-compliance would be to add exception language to Requirement R1 that allows for this.

> NST believes the paragraph titled, "External Networks" is confusing at best. We presume the STD's intent is to encourage Entities to implement INSM in high-value networks outside of ESP. While we are inclined to agree it might be worthwhile, we believe that by virtue of being beyond the scope of CIP-015, it should be omitted.

Likes 0	
Dislikes 0	

Response

Thank you for your comments and for pointing out these statements.

For (1) and (2). We will discuss the addition of a statement such as “it is the opinion of the DT” in those sections.
For (3) the DT intends to specify that an INSM system that provides any form of anomaly detection is a compliant system. This wording and other similar language in the TR is designed to remove ambiguity during audits where the tool selection might be brought into question based on the technology used by the tool. FERC Order No. 887 specifies that the Reliability Requirement be “technology neutral” (Paragraph 77) and this language is included in the TR to ensure that any detection algorithm used by the Responsible Entity is compliant with R1 Part 1.2.

Regarding adding exception language, we’ve discussed exceptions at length several times and each time concluded that we do not want to increase compliance burden for the Responsible Entities. If we add exception language, then entities must demonstrate compliance to the

exception and spend resources on activity that does nothing to improve reliability or detect threats. Suppressing and tuning of alerts is a common daily activity and does not justify additional CIP paperwork that might come under audit scrutiny. The "External Networks" paragraph is specifically related to networks where data is shared to and from an ESP, such as ICCP networks, turbine monitoring networks (e.g. GE M&D). We've changed the heading to "partner networks" and made significant changes. These networks are very high value, and we want to ensure that the intent is clear.
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF notes that the phrase "detecting anomalous or unauthorized activity" in section R1 is of concern as the use of the word "unauthorized" implies a program to authorize network level activity within the ESP. As a network level monitoring standard, entities will need additional context of system monitoring (such as logs) or other data (e.g., work orders for adding new devices to a network) to determine "unauthorized activity" from a detected anomaly. Also, with an "or" between them, an entity can monitor for only unauthorized	

and ignore anomalous traffic. As unauthorized activity is a subset of anomalous activity, we suggest striking “or unauthorized”. It is also noted that requirement part 1.2 only mentions “anomalous network activity” and this would align it with the remainder of the sub-requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT revised Requirement R1 and removed “or unauthorized” from the requirement.	
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 comment.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE reiterates its concerns that this standard would be a challenge to audit and enforce consistently. In Requirement R1, the phrase “based on network security risk(s)” is vague and does not include criteria establishing the network security risks, which could lead to Parts 1.2	

and 1.3 not being relevant. Second, Requirement R3 does not specify how an entity should determine the retention periods, thus leading to a vague requirement.	
Likes 0	
Dislikes 0	

Response

Thank you for your comment.

For R1, the current draft has the language “Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications”…the DT believes that this will allow entities to customize their monitoring locations and to have a documented rationale for why those locations were chosen for audit defense.

In regard to Requirement R3: The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	
Document Name	
Comment	

SMUD recommends the Standards Drafting Team (SDT) change the language in Requirement R1, Part 1.2 so that it is consistent with Requirement R1.

Requirement R1 states "Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of *detecting anomalous or unauthorized network activity*."

Requirement R1, Part 1.2 states "Implement one or more method(s) to *detect anomalous network activity* using the data collected at locations identified in Part 1.1."

Although this inconsistency is minor, the SDT has the opportunity to make the change now and improve the quality of this Standard. This language change is non-substantive and could be made for the final ballot posting.

Likes 0	
Dislikes 0	
Response	

Thank you for your comment. The DT agrees and revised Requirement R1 and its Parts for consistency and clarity.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer	
Document Name	
Comment	

We support TFIST comments

Likes 0	

Dislikes 0	
Response	
Thank you for your comment. Please see responses to TFIST's comments.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC appreciates the SDT addressing ATC's comments from the previous round while maintaining and objective approach and commensurate flexibility in the requirement language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	
Document Name	
Comment	
EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	

Answer	
Document Name	
Comment	
Constellation concurs with NAGF's comments. In addition, Constellation wants the DT to provide further guidance on anomalous or for it to be defined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to NAGF's comments.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
ACES would like to thank the SDT for all their hard work and allowing us to provide feedback	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	

Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "NPCC RSC recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to NPCC RSC's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	

ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
The Technical rational is well written with a lot of detail, however this document from my understanding will not be part of the audit. I would like to see more in the measures, as a high-level for better understanding. Leaving it up to the entities, may still become audit bait, unless	

each entity writes up their rational. The standard is written a Subjective standard vs. an objective standard, this leaves it up to the entity to decide what to audit it on.

The definition anomalous activity needs to be defined; Baseline needs to be defined. Overall, there needs to be a standardized approach for auditing this requirement.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction : PARADOXICAL

Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	
Comment	
The VSLs are too high for R2/R3 compared to R1. Maintaining full logs that only went back 82 days (vs 90) is potentially as or more severe than having a program in place at all (R1). The drafting team should consider a higher VSL for R1 as compared to a lower VSL for R2 & R3 as currently written.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT considered your comment, but decided to make no change to the VSLs.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).	

Kelly Bertholet – Manitoba Hydro

Question 1 -Yes
Comments: Manitoba Hydro supports this change as the previous conditional inclusions were a source of confusion for many.
Response: Thank you for your support.

Question 2 -Yes
Response: Thank you for your support.

Question 3 -Yes
Comments: Manitoba Hydro supports this clear direction.
Response: Thank you for your support.

Question 4 -Yes
Response: Thank you for your support.

Question 5 -Yes
Comments: Manitoba Hydro agrees with this approach, which is clear in its intent. However, there is a concern that the phrase "detecting anomalous or unauthorized network activity" in R1 does not align well with Parts 1.2 and 1.3. We recommend striking "or unauthorized" in R1 to better align with the rest of the standard and avoid confusion as to whether this criteria is "one or the other" or referring to detecting both anomalous and unauthorized network activity. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.
Response: Thank you for your support. The DT has removed "or unauthorized" and has revised Requirement R1 and its Parts for clarity and consistency.

Question 6 -Yes
Response: Thank you for your support.

Question 7 -Yes
Response: Thank you for your support.

Question 8 -No
Comments: Manitoba Hydro is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle could be extremely voluminous and overly expensive. Manitoba Hydro believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, Manitoba Hydro suggests modifying R3:Responsible Entity shall implement one or more documented process(es) to retain meta data collected to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.

Response: Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.
Question 9 -Yes
Response: Thank you for your support.

Question 10 -Yes
Response: Thank you for your support.

Question 11 – Comments: Generator Owner was left out of applicability, should be re-added.
Response: Thank you for your comment. Generator Owners have been included in Section 4 Applicability.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-03 Internal Network Security Monitoring

Initial Ballots and Non-binding Poll Open through March 18, 2024

Now Available

Initial ballots and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels for **Project 2023-03 Internal Network Security Monitoring** are open through **8 p.m. Eastern, Monday, March 18, 2024** for the following standard and implementation plan:

- CIP-015-1 – Internal Network Security Monitoring
- Implementation Plan

Following the January 2024 initial ballot and comments received, the DT decided to create a new CIP Reliability Standard. The new CIP Reliability Standard will be reflected in NERC's system as an initial ballot, as it is the first ballot for Reliability Standard CIP-015. Although NERC's system will reflect the posting as an *initial ballot*, this posting is an ***additional ballot*** for Project 2023-03. The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.
Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) 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 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 information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through March 18, 2024

Now Available

A 20-day formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Monday, March 18, 2024** for the following standard and implementation plan:

- CIP-015-1 – Internal Network Security Monitoring
- Implementation Plan

Following the January 2024 initial ballot and comments received, the DT decided to create a new CIP Reliability Standard. The new CIP Reliability Standard will be reflected in NERC's system as an initial ballot, as it is the first ballot for Reliability Standard CIP-015. Although NERC's system will reflect the posting as an *initial ballot*, this posting is an ***additional ballot*** for Project 2023-03. The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.

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.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Ballot Pools

The existing CIP-007-X ballot pool is being used for all of the ballots associated with this project.

- *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

Initial ballots for the standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 12-18, 2024**.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/317)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 IN 1 ST
Voting Start Date: 3/12/2024 12:01:00 AM
Voting End Date: 3/18/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 233
Total Ballot Pool: 256
Quorum: 91.02
Quorum Established Date: 3/18/2024 2:02:18 PM
Weighted Segment Value: 48.52

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	74	1	30	0.448	37	0.552	0	3	4
Segment: 2	7	0.6	1	0.1	5	0.5	0	0	1
Segment: 3	59	1	26	0.51	25	0.49	0	1	7
Segment: 4	10	0.9	7	0.7	2	0.2	0	1	0
Segment: 5	57	1	18	0.375	30	0.625	0	2	7
Segment: 6	42	1	14	0.378	23	0.622	0	2	3
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	4	0.4	1	0.1	0	1	1
Totals:	256	6	100	2.911	123	3.089	0	10	23

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Negative	Third-Party Comments
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Negative	Third-Party Comments
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Alain Mukama		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu	Jay Sethi	None	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		Negative	Third-Party Comments
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		None	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith		None	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Christine Kane		None	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Andrew Smith		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		Negative	Comments Submitted
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Calpine Corporation	Whitney Wallace		None	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG Nuclear LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Negative	Comments Submitted
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Negative	Third-Party Comments
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Invenergy LLC	Colin Chilcoat		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Manitoba Hydro	Kelly Bertholet		Negative	Third-Party Comments
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 256 of 256 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/317)
Ballot Name: Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT
Voting Start Date: 3/12/2024 12:01:00 AM
Voting End Date: 3/18/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 232
Total Ballot Pool: 254
Quorum: 91.34
Quorum Established Date: 3/18/2024 1:44:45 PM
Weighted Segment Value: 66.71

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	74	1	45	0.682	21	0.318	0	4	4
Segment: 2	7	0.6	4	0.4	2	0.2	0	0	1
Segment: 3	59	1	32	0.627	19	0.373	0	1	7
Segment: 4	10	0.9	7	0.7	2	0.2	0	1	0
Segment: 5	57	1	26	0.565	20	0.435	0	3	8
Segment: 6	41	1	22	0.595	15	0.405	0	2	2
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	3	0.3	0	0	0	3	0
Totals:	254	5.8	139	3.869	79	1.931	0	14	22

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Alain Mukama		Affirmative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu	Jay Sethi	None	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		None	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Negative	Comments Submitted
3	Manitoba Hydro	Mike Smith		None	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		None	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Negative	Comments Submitted
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Calpine Corporation	Whitney Wallace		None	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Decatur Energy Center LLC	Megan Melham		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Third-Party Comments
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		Negative	Third-Party Comments
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Third-Party Comments
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Invenergy LLC	Colin Chilcoat		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 254 of 254 entries

BALLOT RESULTS

Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 Non-Binding Poll IN 1 NB
Voting Start Date: 3/12/2024 12:01:00 AM
Voting End Date: 3/18/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 219
Total Ballot Pool: 247
Quorum: 88.66
Quorum Established Date: 3/18/2024 2:29:43 PM
Weighted Segment Value: 47.54

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	72	1	27	0.491	28	0.509	11	6
Segment: 2	7	0.4	0	0	4	0.4	2	1
Segment: 3	57	1	22	0.524	20	0.476	7	8
Segment: 4	10	0.9	7	0.7	2	0.2	1	0
Segment: 5	55	1	16	0.39	25	0.61	7	7
Segment: 6	40	1	12	0.414	17	0.586	5	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0
Segment: 10	6	0.3	3	0.3	0	0	3	0
Totals:	247	5.6	87	2.819	96	2.781	36	28

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		None	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Negative	Comments Submitted
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Iowa Power Cooperative	Kevin Lyons		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Negative	Comments Submitted
1	Duke Energy	Katherine Street		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Alain Mukama		Abstain	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		None	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		Negative	Comments Submitted
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		None	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Christine Kane		None	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Comments Submitted
4	DTE Energy	Patricia Ireland		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		None	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		Negative	Comments Submitted
5	Bonneville Power Administration	Pamela Van Calcar		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Comments Submitted
5	Calpine Corporation	Whitney Wallace		None	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Decatur Energy Center LLC	Megan Melham		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		None	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Negative	Comments Submitted
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		Negative	Comments Submitted
5	National Grid USA	Robin Berry		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	NextEra Energy	Richard Vendetti		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Omaha Public Power District	Kayleigh Wilkerson		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A
5	Pattern Operators LP	George E Brown		Negative	Comments Submitted
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Don Cribb		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
6	AEP	Mathew Miller		None	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman	Brandon Smith	Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Negative	Comments Submitted
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Negative	Comments Submitted
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Negative	Comments Submitted
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		Abstain	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 247 of 247 entries

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024
20-day formal comment period with ballot	02/27/2024 – 03/18/2024

Anticipated Actions	Date
13-day formal comment period with ballot	04/05/2024 – 04/17/2024
5-day final ballot	TBD
Board adoption	TBD

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 – Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include: each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but are not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M2. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

R3. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M3. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Part 1.3.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1 (1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s) (1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.
R2.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented

				process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.
R3.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024
20-day formal comment period with ballot	02/27/2024 – 03/18/2024

Anticipated Actions	Date
~~20-day formal comment period with ballot~~	~~02/27/2024 – 03/18/2024~~
13-day formal comment period with ballot	04/05/2024 – 04/17/2024
5-day final ballot	TBD
Board adoption	TBD

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:** Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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

   ~~4.1.3.~~4.1.4. Generator Owner

~~4.1.4.~~4.1.5. **Reliability Coordinator**

~~4.1.5.~~4.1.6. **Transmission Operator**

~~4.1.6.~~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 ~~Special Protection System (SPS)~~RAS where the ~~SPS~~ 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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the ~~CIP-002-~~ identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring ~~(INSM)~~ of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems ~~(BCS)~~ and medium impact BES Cyber Systems~~BCS~~ with External Routable Connectivity ~~(ERC) within the Responsible Entity's ESPs~~ to provide methods for ~~increase the probability of~~ detecting and evaluating anomalous ~~or unauthorized~~ network activity. The documented process(es) shall include each of the ~~applicable~~ following requirement ~~parts~~Parts~~.~~: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. ~~Identify~~ Implement, using a risk-based rationale, network data ~~collection~~ feed(s) ~~locations and methods, based on the network security risk(s),~~ to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data ~~collected~~ feed(s) ~~at locations identified in~~from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine ~~appropriate~~ further action(s).

M1. Evidence must include: each of the ~~applicable~~ documented process(es) that collectively include each of the ~~applicable~~ requirement ~~parts~~Parts in Requirement R1 and additional evidence to demonstrate implementation of the process(es). ~~as described in the measure parts.~~ Examples of evidence of implementation of the requirement Parts may include, but are not limited to~~, one or more of the following for each Part~~:

Part 1.1.

- ~~Architecture documents or other documents~~Documentation detailing network data ~~collection~~ feed(s) that includes a documented risk-based ~~methods; or~~
- ~~Documented~~ rationale that describes~~on~~ how network ~~locations~~ data feed(s) were selected for data ~~or excluded for data~~ collection.

Part 1.2.

- Documentation of anomalous network ~~Detection~~ detection events;
- Documentation of ~~Configuration~~ configuration settings of ~~INSM~~ internal network security monitoring systems; ~~or~~
- Documentation of ~~a~~ network communication baseline used to detect anomalous ~~monitor against unauthorized~~ network activity~~.~~; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response~~s~~ to detected anomalies~~, etc.~~; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification~~, except during CIP Exceptional Circumstances~~. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M2. ~~Examples of evidence~~ Evidence may include, but ~~are~~ is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

R3. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring ~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3~~and other meta-data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances~~. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M3. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Part 1.3.~~perform the analysis of actionable anomalous activity.~~

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from ~~collected at locations identified in~~ Part 1.1 (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine ~~appropriate~~ further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement ~~parts~~ Parts for detecting and evaluating anomalous network activity~~to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3)~~. ~~OR~~ ~~The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1).~~
R2.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional

				Circumstances, implement one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification. ~~(except during CIP Exceptional Circumstances).~~
R3.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring ~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3~~and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances)~~.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC)[2]. INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address three security issues.

[1] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] *Id.* P 5. (Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment) and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices).

In Order No. 887, FERC directs NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

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 thirty-six (36) 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.

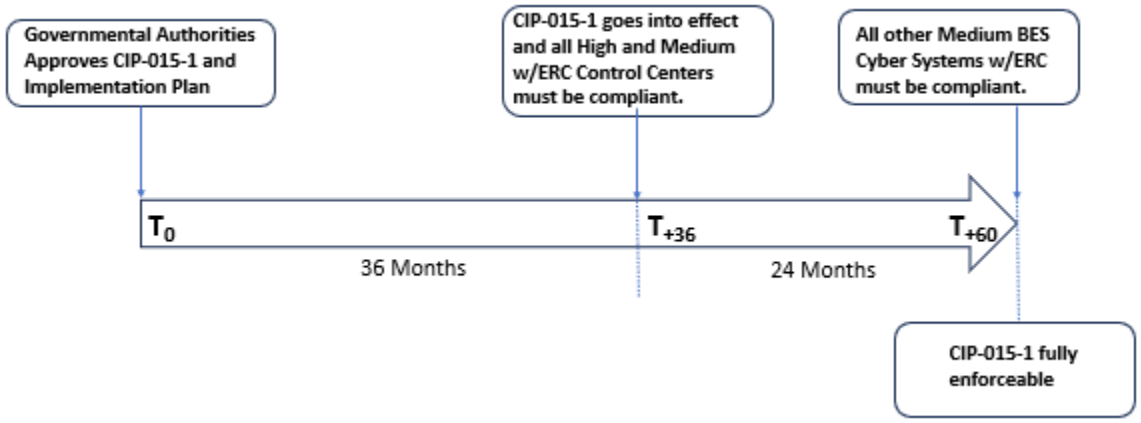
Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1. and R1.2. shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It further

accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC).[2] INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address ~~the~~ three security issues.[3] In Order No. 887, FERC direct~~ed~~s NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

[1] *See* Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[3] *Id.* P 5. (Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment)~~;~~

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

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 thirty-six (36) 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 thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

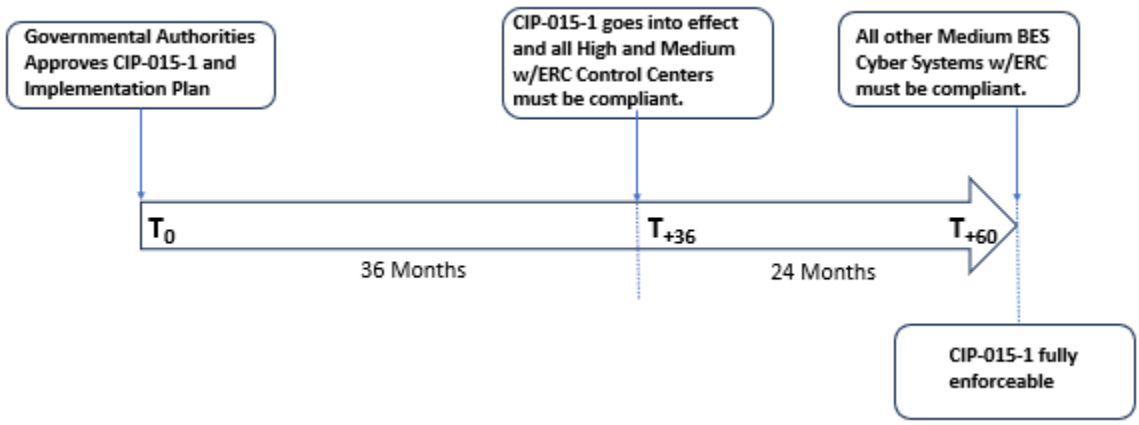
Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1. and R1.2. shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability

and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices).

Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2023-03 Internal Network Security Monitoring

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2023-03 INSM/CIP-015-1 – Internal Network Security Monitoring** by **8 p.m. Eastern, Wednesday, April 17, 2024.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Laura Anderson, or at 404-782-1870.

Background Information

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for Internal Network Security Monitoring (INSM) of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard requirements for any new or modified CIP Reliability Standards that address three security issues.[2] In Order No. 887, FERC directs NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

The Project 2023-03 Drafting Team (DT) developed Draft 2 of proposed CIP-015-1 that requires Responsible Entities to implement a Network Security Monitoring (NSM) system. Responsible Entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks.

INSM refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the trusted CIP related operational zones of the responsible entity.

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *See id.* P 5.

Order No. 887 included the phrase "CIP-Networked Environment," which was not specifically defined in Order No. 887, INSM. In the initial posting, the DT included in its proposed revisions communications between EACMS and PACS outside of the ESP as part of the CIP-Networked Environment.

Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of Electronic Access Control and Monitoring System (EACMS) and Physical Access Control Systems (PACS) outside of the ESP. The DT made this decision based upon: (1) industry overwhelmingly agreeing that the order was not broad enough to include EACMS and PACS outside of the ESP within the scope of Project 2023-03; and (2) the inclusion of EACMS and PACS introduced a number of difficult technical complications, e.g., the need to define CIP-Networked environment and how to facilitate the technical inclusion of EACMS and PACS.

At the start of Project 2023-03, INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of Reliability Standard CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align as well with the objectives of Project 2023-03. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

General changes from Draft 1 of Reliability Standard CIP-015-1:

- Generator Owner was added to the Section 4 Applicability Section.
- References to Special Protection System (SPS) changed to Remedial Action Scheme (RAS)[3]
- Requirement R1:
  - Concept of "within ESP" was changed to "…protected by…"
  - "…or unauthorized…" removed, as it implies authorization process
  - "…increase the probability of…" to "…provide methods for," to remove subjectivity of the phrase
  - Network data collection "locations and methods" revised to "feed(s)"
    - Revisions were in response to comments indicating concerns about having to document physical locations
  - "…based on network security risks…" changed to "…using a risk-based rationale…"
- Requirement R2:
  - "…and data retained in support of Requirement R3…" was added to Requirement R2 to clarify that retained internal network security monitoring data needs to be protected
- Requirement R3
  - Clarified data retention requirements
  - Added a note following the requirement, ensuring that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected

[3] In a Letter Order issued on June 23, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," to "See "Remedial Action Scheme"". This change effectuated NERC's proposed transition from the term "Special Protection System" to the newly revised term "Remedial Action Scheme (RAS)." *See N. Am. Elec. Reliability Corp.,* Docket No. RD16-5-000, at p. 2 (June 23, 2016).

Questions

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

   ☐ Yes
   ☐ No

   Comments:

5. Please provide any additional comments for the DT to consider, if desired.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es). Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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	The proposed VSL is binary. It does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-015-1, Requirement R2	
Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSL is binary. It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement one or more documented process(es) for ~~INSM~~ internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems ~~(BCS)~~ and medium impact BES Cyber Systems~~BCS~~ with External Routable Connectivity ~~(ERC) within the Responsible Entity's ESP~~ to provide methods for ~~increase the probability of~~ detecting and evaluating anomalous ~~or unauthorized~~ network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though~~While~~ the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es)~~., the VRF is reflective of the implementation as a whole.~~ Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from ~~collected at locations identified in~~ Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine ~~appropriate~~ further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement ~~parts~~ Parts ~~to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3)~~for detecting and evaluating anomalous network activity. ~~OR~~ ~~The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1).~~

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification~~, except during CIP Exceptional Circumstances~~. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification ~~(except during CIP Exceptional Circumstances)~~.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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	The proposed VSL~~s are~~ is ~~not b~~inary. ~~and do~~It does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-015-1, Requirement R2	
Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 except during CIP Exceptional Circumstances.~~ Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring ~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances).~~

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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 VSL~~s are not~~is binary. ~~and do~~It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address three security objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of networks that are internal to the operational zones of the Responsible Entity. While the Responsible Entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following

3 security objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices that are protected by the ESP of applicable BES Cyber Systems.

Reliability Standard CIP-015-1 requires Responsible Entities to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the collection location(s) and method(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to anomalous suspicious network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation could include escalation to a Responsible Entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. INSM will be an on-going, or possibly an iterative, process enabling Responsible Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887, schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Creation of new Standard CIP-015

At the start of Project 2023-03 - INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

[3] NERC Glossary of Terms
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with our objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification

The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[6]" should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM

The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.*

Summary

Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the Responsible Entity for network monitoring purposes.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

[6] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

As described in Richard Bejtlich's book, “The Practice of Network Security Monitoring”, monitoring is most effective when collection is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods (Chapters 9-11). In “Applied Network Security Monitoring” (Chris Sanders, Jason Smith), the “Applied Collection Framework” is described wherein Responsible Entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1. specifies that the Responsible Entity identify possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ESP networks and select and implement a collection of INSM network data feed that provides the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity’s evaluation of the network cyber security risk in their internal networks.

Data Collection Locations

In Reliability Standard CIP-015-1, "network data feed(s)" refers to both a physical and a logical concept. In a physical context, network data collection locations connote data collection from devices that perform technical functions within and between networks such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. A Responsible Entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the Responsible Entity may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

The Responsible Entity is responsible for identifying physical and logical network data feed(s) that will provide the highest value data for the INSM system.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments. High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.

"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Considerations for selecting Network Data Feeds

The following considerations might inform the decision for collecting data from a network data feed:

Adversary Analysis

The Responsible Entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive collection priorities to focus on targeted uses cases that would inform collection locations and exclusions.

ICS Protocols

The collection locations and methods, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyze ICS specific protocols.

Data Types

The MITRE ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting data locations and methods, a Responsible Entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network collection locations and methods. Consideration of traffic duplication may be part of a rationale on how network locations were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection

capabilities of other installed systems should be considered when narrowing the focus of network data collection locations.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network locations were selected or excluded for data collection.

A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Part 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alerts in some INSM systems. Suppressing alarms or collections may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.
2. High rates of false positive alerts until tuning can be completed.
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the DT these common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

Partner Networks

Transmission Operators have connections to partner networks for the purpose of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some Generator Operators implement connections to external partners for turbine monitoring systems. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value for INSM data collection.

Resilience

While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some

control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1. allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN
Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering
Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection
Requirement R1, Part 1.1. does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability
Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a “per system capability” exclusion, Requirement R1, Part 1.1. allows wide latitude to identify INSM data collection locations and data collection methods appropriate to each Responsible Entity’s ESP networks.

Some networks may not have the capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity has several options to provide monitoring data to the INSM including:

- Upgrading hardware and software to systems that do have the capability.
- Installing TAPs to collect network data.
- Collecting flow data.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity.

- Supplementing network data feeds with other pertinent data feeds such as endpoint logs and firewall logs.
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[7].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities are not expected to implement all of these, but rather to choose and implement the collection locations and methods that provide the most value to the Responsible Entity, as determined by the risk-based rationale in Requirement R1, Part 1.1.

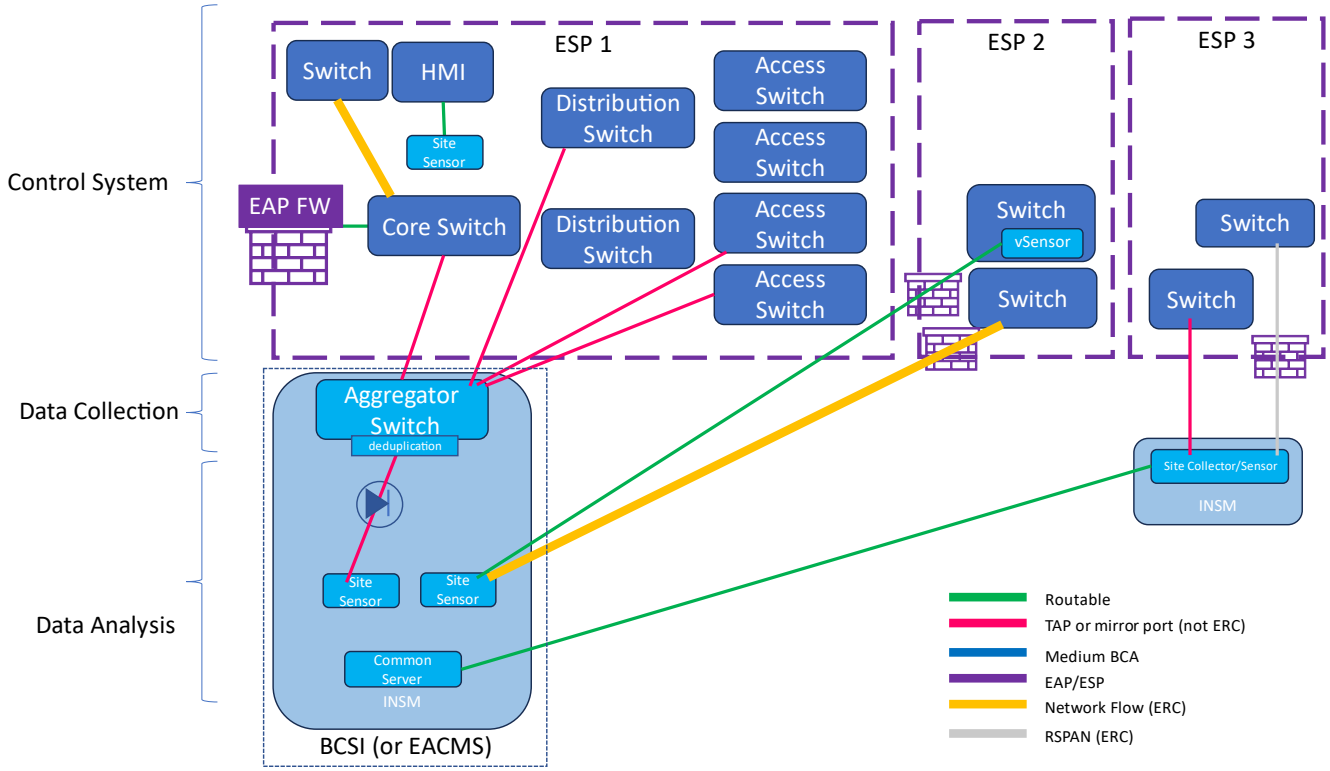


Figure 1

This reference architecture in Figure 1 has the following features:

ESP1

[7] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of technology advancements, new anomalous detection products are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and the INSM Requirement R1 and Requirement R1, Part R1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by

itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

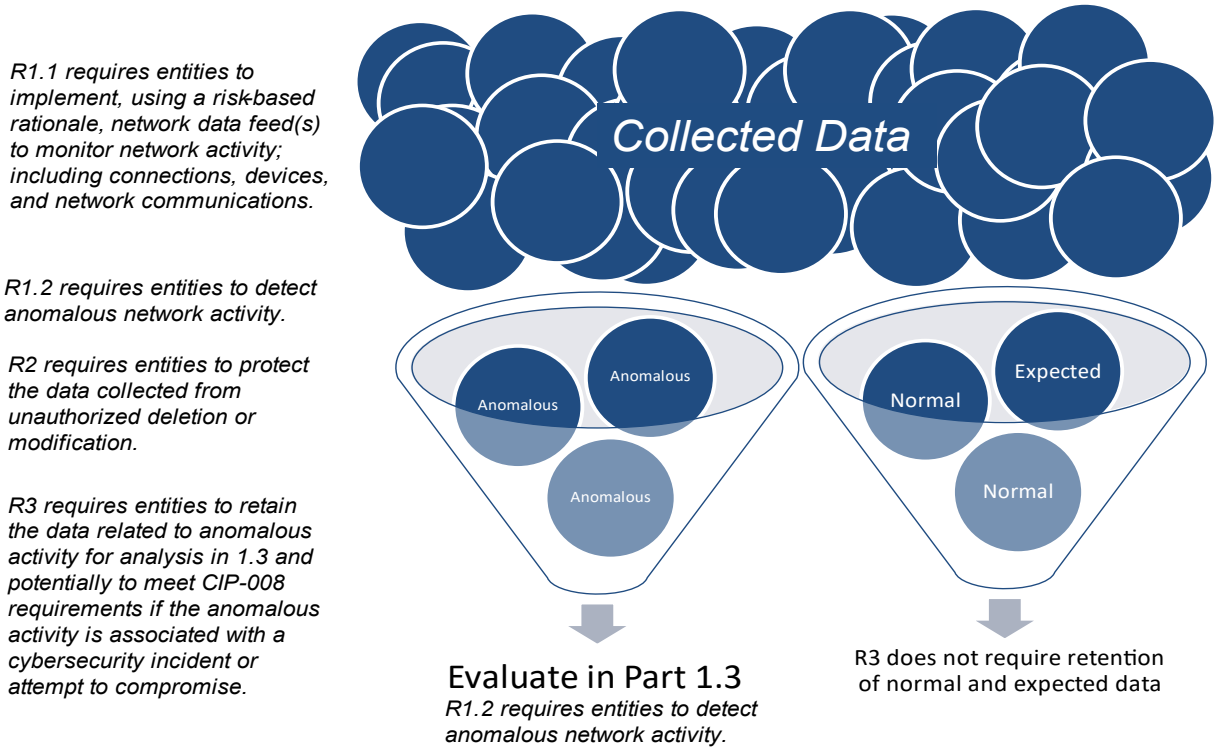


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Signature-based detections
Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.
When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for data retention in Requirement R2.

Behavioral Detections
Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[8] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning
After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking
INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods
Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods
As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).

[8] https://attack.mitre.org/techniques/T0888/

- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning
Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[9] book. Analyzing the data is an expected part of cyber security operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[9] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

Rationale for Requirement R2

Requirement R2: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[10]). The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system.
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Rationale for Requirement R3

Requirement R3: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3."

Requirement R3 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide evidence needed to meet CIP-008-6 Requirement R3 for data retention related to an actual Cyber Security Incident or attempt to compromise.

[10] https://attack.mitre.org/techniques/T1070/

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system.

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement R2 is intended to limit information sharing. The focus of Requirement R2 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities to share information gathered by INSM systems (see NIST 800-150[11], CISA Information Sharing Guidance[12], Cyber security Information Sharing act of 2015[13]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[14]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities may need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

[11] https://csrc.nist.gov/pubs/sp/800/150/final
[12] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[13] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[14] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feeds to implement as part of Requirement R1, Part 1.1.

The table below uses the following simplified diagram of a high impact ESP network.

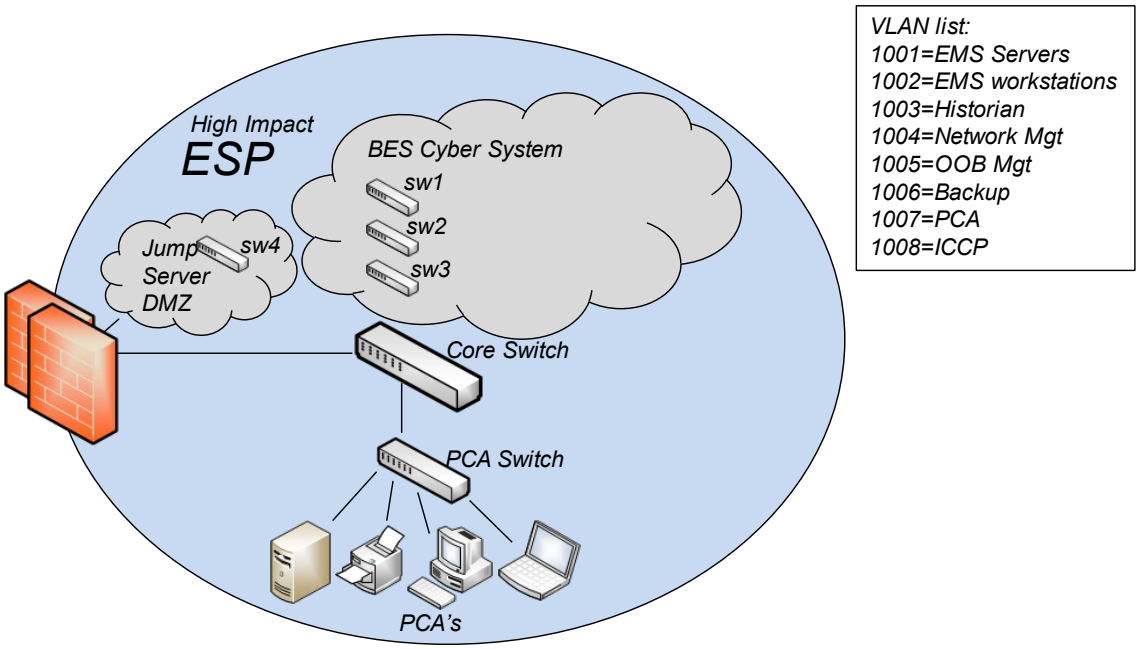


Figure 3

Example rationale for selecting Network Data Feeds:

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports	IRA to the jump server is a likely attack vector.

			to physical port	
	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected

				to be abused by a malicious insider. The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.

This example provides some of the considerations for selection network data feeds. This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.

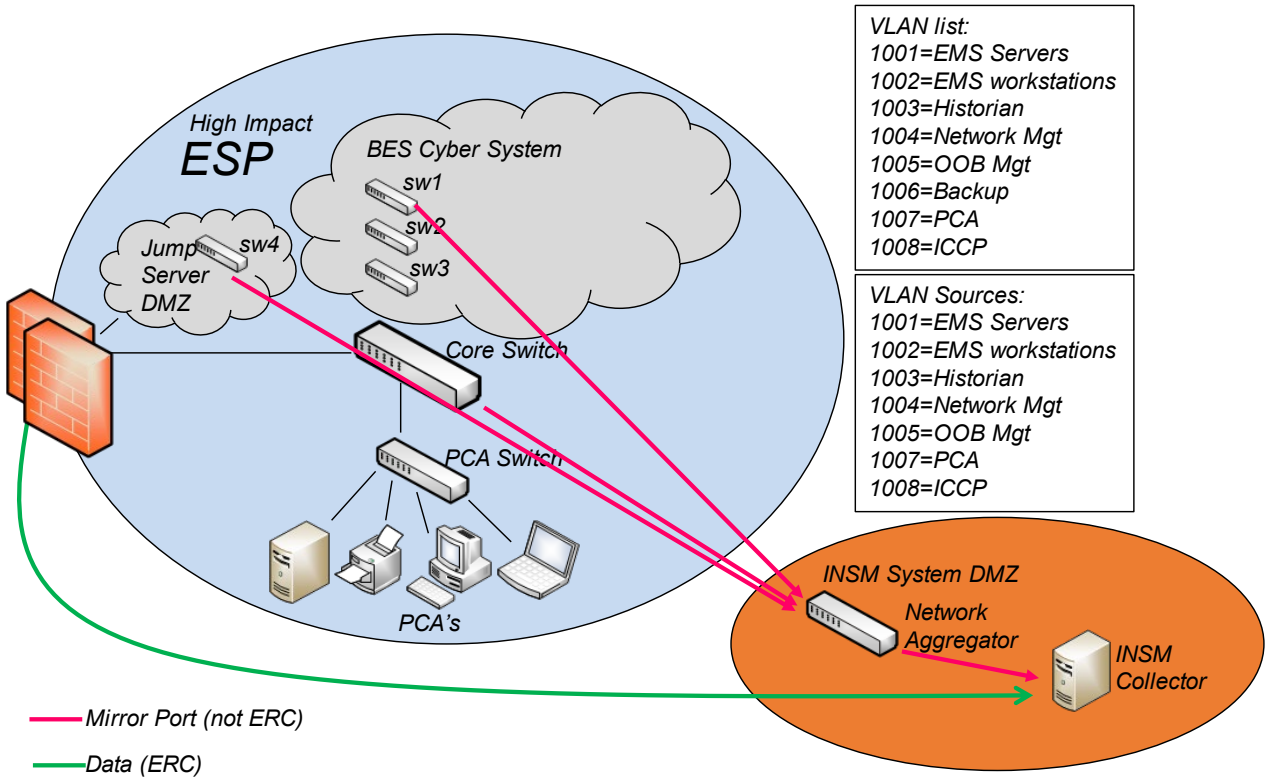

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities~~entities~~ to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 ~~directs~~ directed NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address ~~the~~ three security ~~issues~~objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats ~~and incidents.~~. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of ~~systems~~networks that are internal to the operational zones of the Responsible Entity. While ~~the~~ Responsible Entities~~entities~~ may choose to use

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following 3 security ~~issues~~objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices ~~within~~that are protected by the ESP of applicable BES Cyber Systems.

~~The Project 2023-03 DT proposed~~ Reliability Standard CIP-015-1 requires Responsible Entities ~~responsible entities~~ to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the collection location(s) and method(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to ~~unexpected,~~ anomalous~~, or otherwise~~ suspicious network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation ~~That~~ could include escalation to a~~n~~ Responsible Entity~~entity~~'s CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data ~~and metadata~~ to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. ~~In addition, entities must retain relevant data collected from their INSM system(s) with sufficient detail and duration to facilitate the evaluation and further investigation of potential cybersecurity incidents.~~ INSM will be an on-going, or possibly an iterative, process enabling ~~responsible~~ Responsible ~~entities~~ Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The ~~Drafting Team~~DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. ~~The options included addition of INSM requirements to the CIP standards' framework.~~ The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887[4], schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[5] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[6].

Creation of new Standard CIP-015

[3] NERC Glossary of Terms
[4] ~~*Id.*~~
[5] Bejtlich, Richard; *The Practice of Network Security Monitoring*; published by No Starch press; June 15, 2013.
[6] Sanders, C., Smith, J., and Koh, E.J.; *Applied Network Security Monitoring: Collection, Detection, and Analysis*; Syngress Publishing; December 2013.

At the start of Project 2023-03, - INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the review of the ssubsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with our objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new Rreliability Sstandard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and

existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification
The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[7]" should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM
The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as ~~Endpoint Detection~~endpoint detection and ~~Response~~response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While ~~an entity~~a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not ~~expected or~~ required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Responsible Entity shall implement one or more documented process(es) for internal network security monitoring ~~(INSM)~~ of networks protected by the Responsible Entity's Electronic Security Perimeters~~ESP(s)~~ of high impact BES Cyber Systems ~~(BCS)~~ and medium impact BES Cyber Systems~~BCS~~ with External Routable Connectivity ~~(ERC)~~ to provide methods~~-~~ for detecting and evaluating anomalous network activity.*

Summary
Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ~~ protected by~~ ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities ~~Registered Entities~~ create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the~~ a~~ Responsible Entity ~~registered entity~~ for ~~cybersecurity~~network monitoring purposes.

Rationale for Requirement R1 Part 1.1

[7] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Requirement R1, Part 1.1: "~~Identify~~Implement, using a risk-based rationale, network data ~~collection locations and methods that provide value, based on the network security risk~~feed(s~~),~~) to monitor network activity~~;~~ including connections, devices, and network communications~~.''~~."

As described in Richard Bejtlich's book, "The Practice of Network Security Monitoring~~,~~", monitoring is most effective when collection ~~occurs~~is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods~~.~~ (Chapters 9-11). In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein Responsible Entities ~~entities~~ first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1 ~~requires~~specifies that the Responsible Entity ~~Registered Entity to~~ identify ~~many~~ possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity ~~Registered Eentity~~ might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks~~,~~ and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ~~internal~~ ESP networks and select ~~an INSM data~~ and implement a collection ~~location(s) and method(s)~~of INSM network data feeds that provide the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that ~~provides~~provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.

Data Collection Locations

In Reliability Standard CIP-015-1, "network data ~~collection locations~~feed(s)" refers to both a physical and a logical concept. In a physical context, network data collection locations connote data collection from devices that perform technical functions within and between networks~~,~~ such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity~~entity~~ could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. ~~a~~ The Responsible Entity ~~An entity~~ may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the Responsible Entity ~~an entity~~ may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host

by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

The ~~entity~~ Responsible Entity is responsible for identifying physical and logical ~~communication convergence points~~network ~~locations~~data feed(s) that will provide the highest value data for the INSM system.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network ~~TAPs~~test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require~~Usually not~~ ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities ~~responsible entities~~ will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an ~~EAP.~~Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. ~~Capable of performing in low bandwidth environments.~~ Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports.

	Most sensors require external data collection technology to gather data. Hardware costs are can be high. Relatively fast deployment in centralized environments. High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Optional considerationsConsiderations for selecting or excluding collection locations and methodsNetwork Data Feeds

As entities determine collection locations and methods theThe following considerations might inform the decision for including or excludingcollecting data from a collection location or methodNnetwork Ddata Ffeed:

Adversary Analysis

The Responsible Entityentity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive collection priorities to focus on targeted threats and uses cases that would inform collection locations and exclusions.

ICS Protocols

INSM technologies are most meaningful and effective when they are built to be ICS protocol aware and provide detections of network activity that might hamper an industrial process. The collection locations and methods, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyzedetect ICS specific attacksprotocols.

Data Types

The MitreMITRE ATT&CK framework, describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting data locations and methods, a Responsible Entityan entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network collection locations and methods. Consideration of traffic duplication may be part of a rationale on how network locations were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data collection locations.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network locations were selected or excluded for data collection.

~~An entity with mature firewall logging capabilities and extensive segmentation~~A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the ~~drafting team~~DT, does not ~~a~~constitute cause for ~~potential~~ non-compliance with Requirement R1, Part 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM collection capability~~system components~~ and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of ~~alarms~~ alerts in some INSM systems. Suppressing alarms or collections may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.~~;~~
2. High rates of false positive alerts until tuning can be completed.

3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the Drafting teamDT these common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

ExternalPartner Networks

External networks, such asTransmission Ooperators have connections to partner networks for purposes of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some generationGenerator Ooperators implement connections to external partners for turbine monitoring systems, ICCP connections, etc.,. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value networks for INSM data collection of data related to these functions is more likely to be selected than excluded from network data collection.

Resilience

While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1 allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN

Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering

Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally resultresults in higher signal to noise ratios and better detection outcomes.

Out of Scope collection

Requirement R1, Part 1.1 does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.

- Wide area network circuits such as ~~MPLS~~multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability

Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a "per system capability" exclusion, Requirement R1, Part 1.1 allows wide latitude to identify INSM data collection locations and data collection methods appropriate to each Responsible Entity~~entity~~'s ESP networks.

Some networks may not have capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity ~~Registered Entity~~ has several options to provide monitoring data to the INSM system including:

- Upgrading hardware and software to systems that do have the capability~~,~~.
- Installing TAPs to collect network data~~,~~.
- Collecting flow data~~,~~.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity~~,~~.
- Supplementing network data feeds with other pertinent data feeds such as endpoint logs ~~and~~or firewall logs~~,~~. ~~and~~
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity ~~Registered Entity~~ would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[8].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities ~~Entities~~ are not expected to implement all of these, but rather to choose and implement the collection locations and methods that provide the most value to the Responsible Entity~~entity~~, as determined by the risk-based rationale in Requirement R1, Part 1.1.~~,~~

[8] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

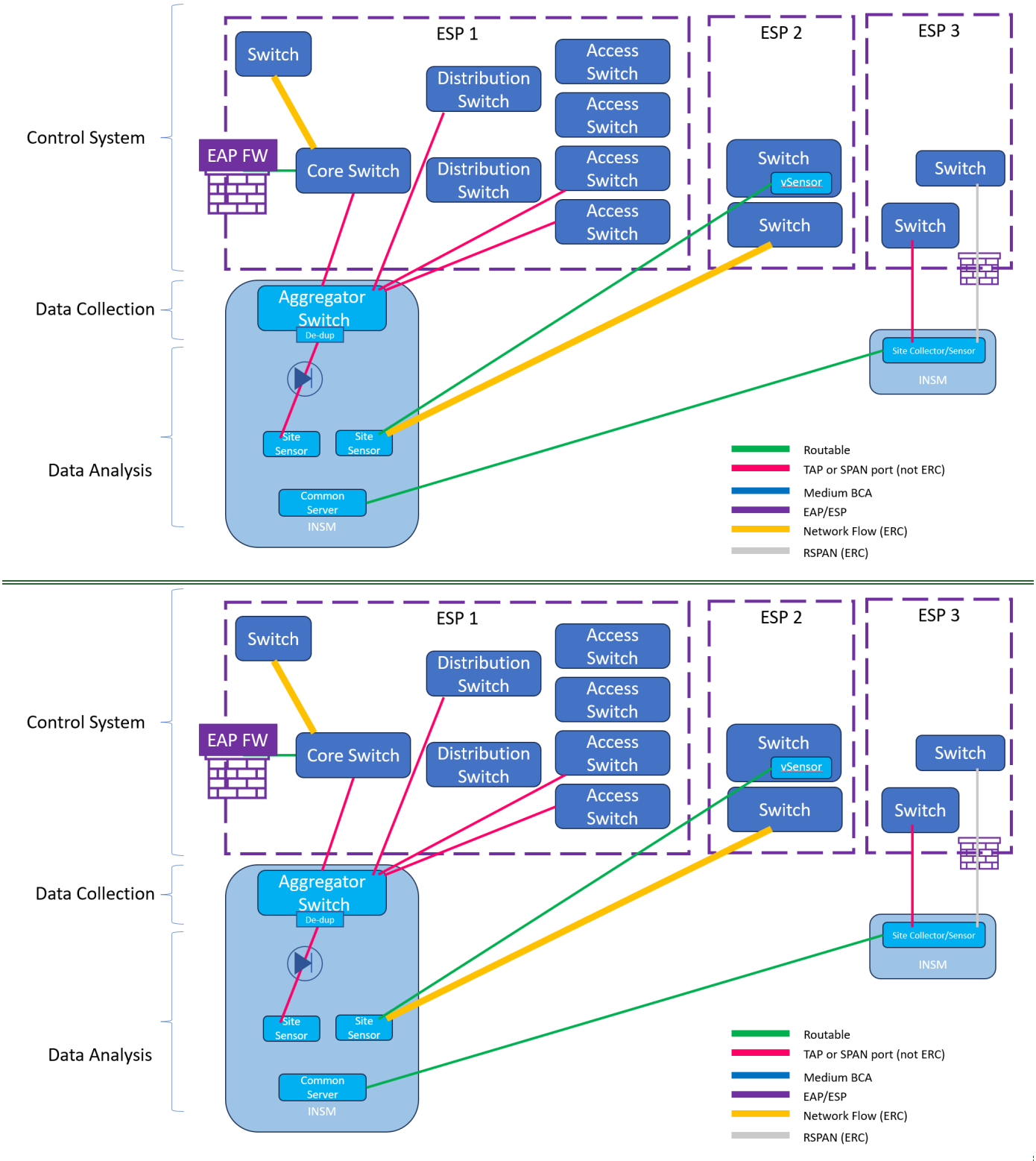

Control System
Data Collection
Data Analysis
ESP 1
ESP 2
ESP 3
Switch
EAP FW
Core Switch
Distribution Switch
Distribution Switch
Access Switch
Access Switch
Access Switch
Access Switch
Switch
vSensor
Switch
Switch
Switch
Aggregator Switch
De-dup
Site Sensor
Site Sensor
Common Server
INSM
Site Collector/Sensor
INSM
Routable
TAP or SPAN port (not ERC)
Medium BCA
EAP/ESP
Network Flow (ERC)
RSPAN (ERC)

Figure 1

This The reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As we witness a result, of the rise of AI on the technology landscapeadvancements, with we will likely see new anomalous network activity detection products that use AI learning models are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity an entity uses to comply with the requirements. The goal is for entitiesResponsible Entities is to be able to detect adversaries within ESP networks. Determining what technology each entityResponsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

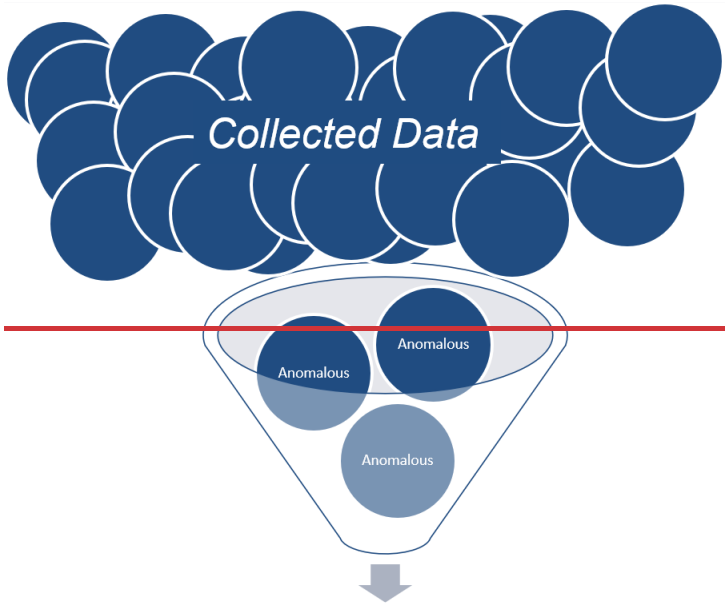
Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified innetwork data feed(s) from Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and the INSM Requirement R1 and Requirement R1, Part R1.2, “anomalous” refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word “anomalous” or “anomaly” in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as “anomaly detection.” Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the ~~entity~~Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.



Evaluate in Part 1.2

R1.1 requires entities to implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

R1.2 requires entities to detect anomalous network activity.

R2 requires entities to protect the data collected from unauthorized deletion or modification.

R3 requires entities to retain the data related to anomalous activity for analysis in 1.3 and potentially to meet CIP-008 requirements if the anomalous activity is associated with a cybersecurity incident or attempt to compromise.

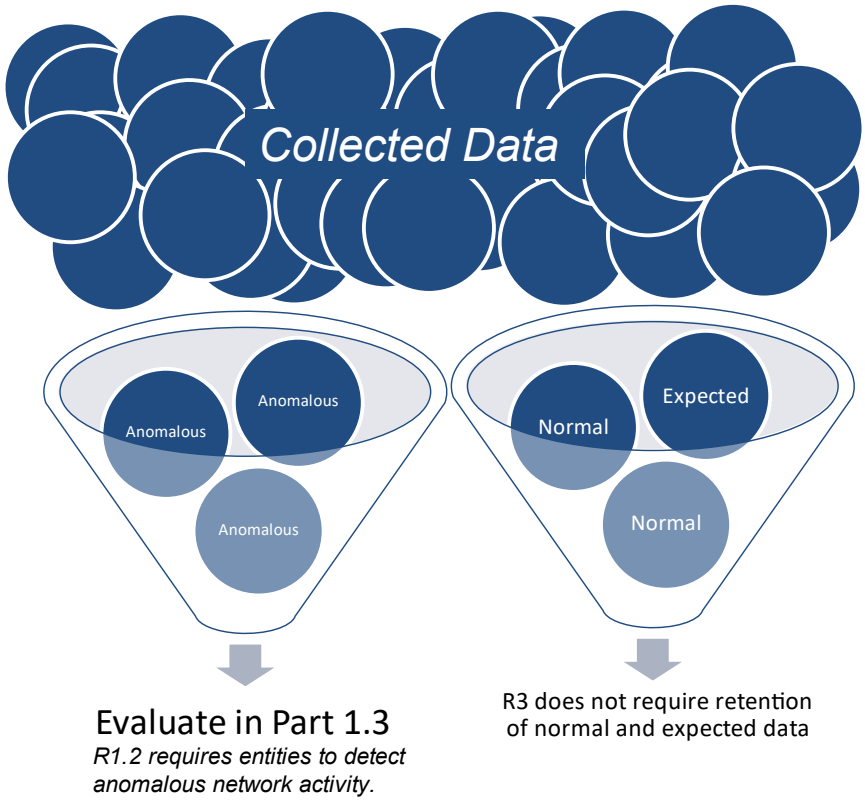


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the ~~entity's~~Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. ~~baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.~~ Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

~~Anomaly detection is sometimes referred to using other names such as modeling.~~ ~~Products may include machine learning algorithms and other technology to reduce the number of notifications.~~

Signature-based detections

Signature-based detection is a technique used by ~~Intrusion Detection Systems, Deep Packet Inspection~~intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.

When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for ~~metadata~~ data retention in Requirement R2.

Behavioral Detections

Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[9] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) ~~scanning~~Scanning

After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking

INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods

Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods

As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

[9] https://attack.mitre.org/techniques/T0888/

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).
- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

This document cannot contain an exhaustive list of all possible detection methods. The ~~entity~~Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning

Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3~~: "~~. "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine ~~appropriate~~further action~~."~~(s)."

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[10] book. Analyzing the data is an expected part of cyber security operations.

Evaluation

Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity~~an entity~~ has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions

Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities ~~Registered Entities~~ Incident Response ~~plan~~ Plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[10] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

Rationale for Requirement R2

Requirement R2: "Implement Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more method(s documented process(es) to protect the internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[11]). The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls like those used to protect BCSI or EACMS.. Examples of controls that should could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system,
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.,.
- Granting only authorized personnel access to the INSM system.
- Segmentation of the INSM system into an isolated network separate from OT and corporate networks.the BES Cyber System being monitored,.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.,.
- Implement two-factor authentication for access to the INSM system., or.
- Other commonly accepted methods used to protect log data.

Note that no part of Reliability Standard CIP-015-1 or Requirement R2 or is intended to limit information sharing. The focus of Requirement R2 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques and procedures is part of a mature cybersecurity program. Government agencies expect and encourage registered entities to share information gathered by INSM systems (see NIST 800-150[12], CISA Information Sharing Guidance[13], Cybersecurity Information Sharing act of 2015[14]).

The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[15]" states that the CIP-011 Requirement R1, Part 1.2 process "should include how the registered entity addresses providing BCSI to third-party vendors or other recipients." After implementing

[11] https://attack.mitre.org/techniques/T1070/
[12] https://csrc.nist.gov/pubs/sp/800/150/final
[13] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[14] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[15] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

~~INSM entities may need to review their CIP-011 Requirement R1, Part 1.2 process to ensure that it includes a process for sharing INSM data with third-party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.~~

Rationale for Requirement R3

Requirement R3: "~~Implement~~Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain ~~network communications~~internal network security monitoring data ~~and other metadata collected~~associated with ~~sufficient detail and duration~~network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support ~~the analysis in Requirement R1,~~of Part 1.3."

Requirement R3 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide evidence needed to meet CIP-008-6 Requirement R3 for data retention related to an actual ~~cyber~~Cyber ~~security~~ Security ~~incident~~ Incident or an attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity~~Registered Entity~~
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity~~Registered Entity~~

Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity~~Registered Entity~~
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity~~Registered Entity~~
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity~~Registered Entity~~

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. ~~An entity~~ A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system. ~~Specifying retention timeframes as averages or moving targets rather than absolute values is an acceptable specification in a data retention chart.~~

~~Metadata~~

~~In the context of Requirement R3, INSM related metadata is a record of past network communication and traffic or a summarization of that traffic.~~

~~Metadata retention will vary by protocol. For example, some ICS protocols do not use layer 3, and other ICS protocols are layer 3, but do not create TCP connections. The decision and capabilities of what metadata is retained is frequently configured as part of the INSM system. Registered Entities should consult with vendors to ensure that INSM tools store sufficient data to support necessary analysis of network activity.~~ The decision of which metadata to store and retention timeframes should enable the entity to accomplish its cybersecurity and operational objectives.

~~The decision of which metadata to store and retention timeframes should enable the entity to accomplish its cybersecurity and operational objectives.~~

~~Metadata could also include information about the traffic, such as:~~

- ~~Layer 2 traffic, such as:~~
  - ~~ARP;~~
  - ~~ICMP;~~
  - ~~DHCP requests;~~
  - ~~Multicasts;~~
  - ~~Broadcasts;~~
  - ~~Source MAC addresses;~~

- Destination MAC addresses;
- VLAN tags;
- CDP/LLDP; or
- Layer 2 protocol traffic

- Layer 3 traffic, such as:
  - Source IP addresses;
  - Destination IP addresses;
  - Source TCP and UDP ports;
  - Destination TCP and UDP ports;
  - TCP header information; or
  - TCP payload metadata (size, content, determination if encrypted)

- Connection Creation information
  - TCP 3-way handshake; or
  - Connection termination information

- Summarizations of any of the above data
  - In control networks there are devices that send very repetitive data across the networks at high frequency. A summarization of this data is part of a metadata record. For example, a merging unit sending 100 goose messages per cycle on a station bus is an example of communications that might make sense to summarize rather than to store in a raw format or to store only exceptions of the expected traffic, or to not store at all if the entity assesses that retaining the repetitive data is a low cybersecurity value.

- Software and protocol identification
  - Some network communications can be linked to specific software with a high degree of confidence. Examples include telnet, FTP, DNS, SMTP, SNMP, ICMP, and similar unencrypted protocols that have internet RFP standards defined. However, some network communications may require analysis to infer the software being used. It is understood that encrypted payloads using common TCP or UDP ports may be difficult to identify correctly. INSM systems with accurate network communications protocol (software) classification are highly useful for cybersecurity investigations. Responsible Entities are encouraged to use tools that classify the software being used, it is understood that no system will achieve 100% protocol identification accuracy.
- Application Information
    - DNS queries and responses
    - User Agent Strings
    - File Extraction

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement R2 is intended to limit information sharing.

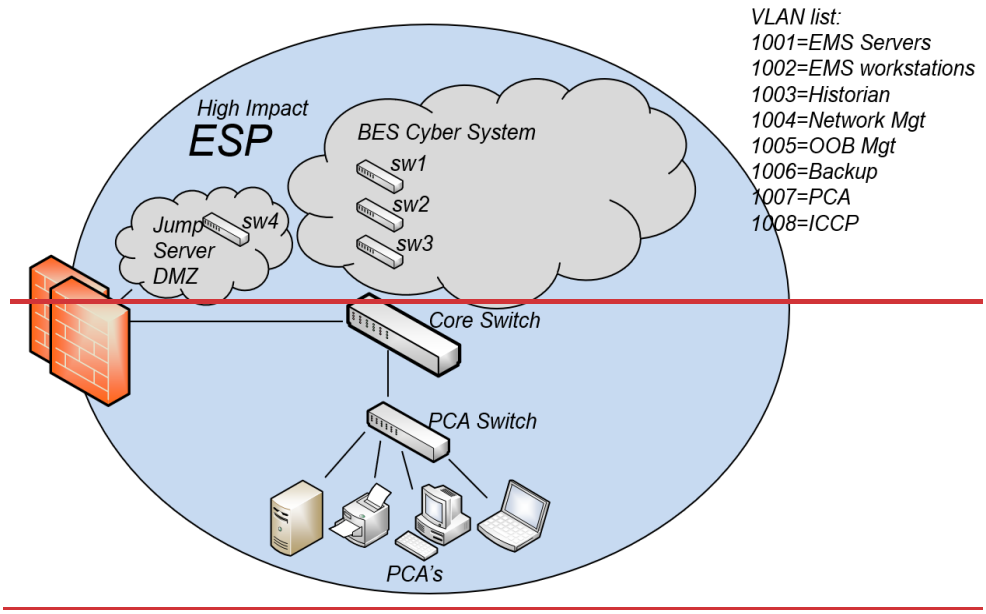
- ~~Network~~ Device Attributes
  - ~~Network data may be used to gather information about devices communicating on the network and may be used to infer or detect information about the device or to enrich asset inventory data. A known INSM limitation is that asset data will not achieve 100% accuracy from passive network analysis.~~

The focus of Requirement R2 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities ~~registered entities~~ to share information gathered by INSM systems (*see* NIST 800-150[16], CISA Information Sharing Guidance[17], Cyber security Information Sharing act of 2015[18]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[19]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity~~registered entity~~ addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities ~~entities~~ may need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

[16] https://csrc.nist.gov/pubs/sp/800/150/final
[17] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[18] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[19] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feed(s) to implement as part of ~~the~~ Requirement R1, Part 1.1.
The table below uses the following simplified diagram of a high impact ESP network.


VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's

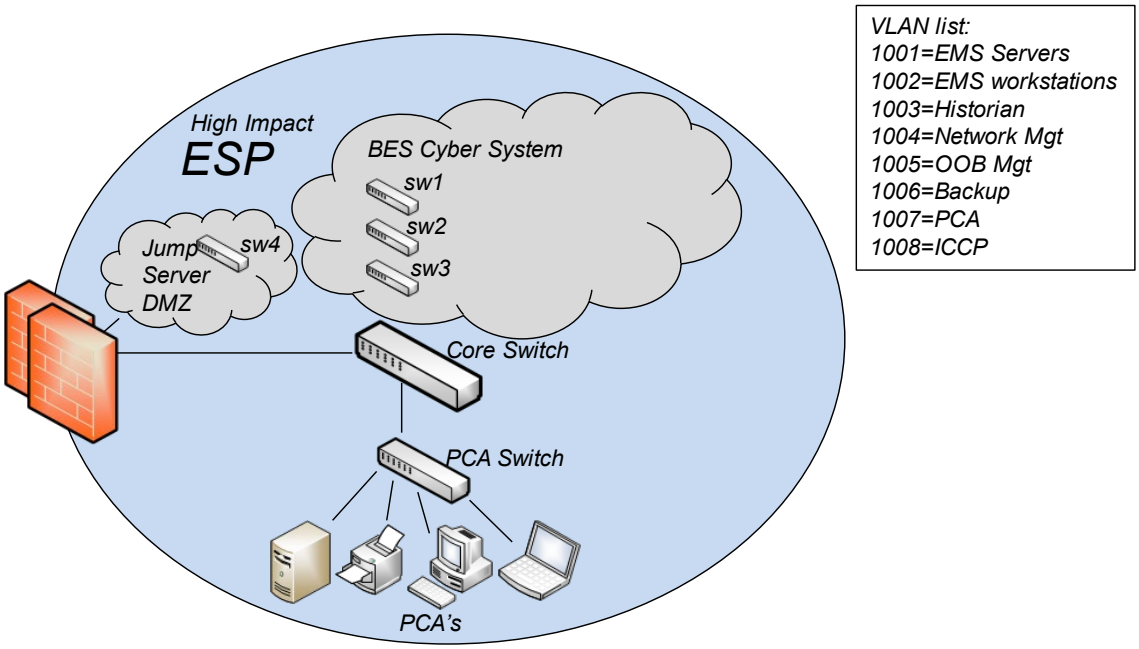

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's

Figure 3

Example rationale for selecting Network Data Feeds:

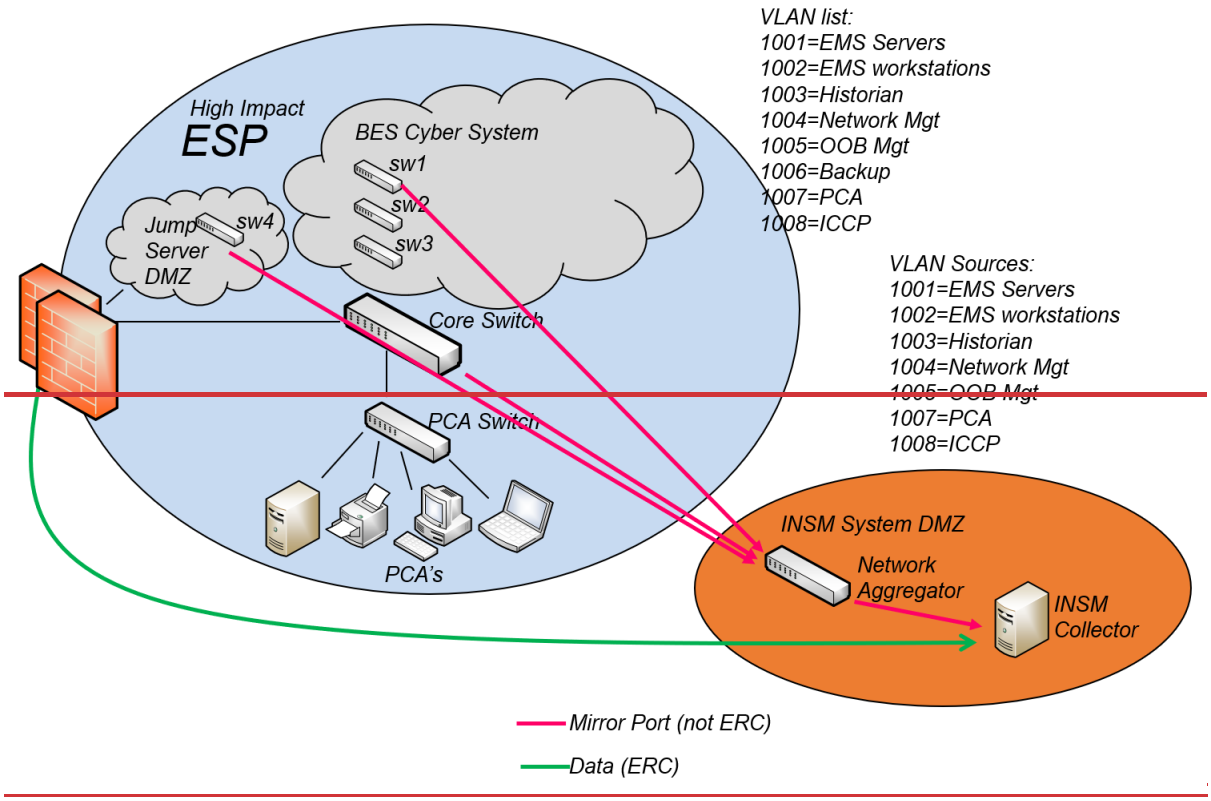
Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports to physical port	IRA to the jump server is a likely attack vector.

	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs ~~is~~are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected to be abused by a malicious insider.

				The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.
~~**Firewall Flow**~~	~~Yes~~	~~ESP Firewall logs~~	~~Netflow Syslog~~	~~Although firewall logs are sent to SIEM, Netflow and syslog are duplicated to INSM because the INSM vendor has an integration with this firewall~~
	~~No~~	~~Firewall Replication Traffic~~		~~This is an internal subnet used only between firewalls for configuration replication. There are no known attacks or alerts in the INSM system so collecting this data would not result in any true positive alerts but might generate false positive alerts that would waste the time of analysts.~~

This example provides some of the considerations for selection of network data feed(s). This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.


VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

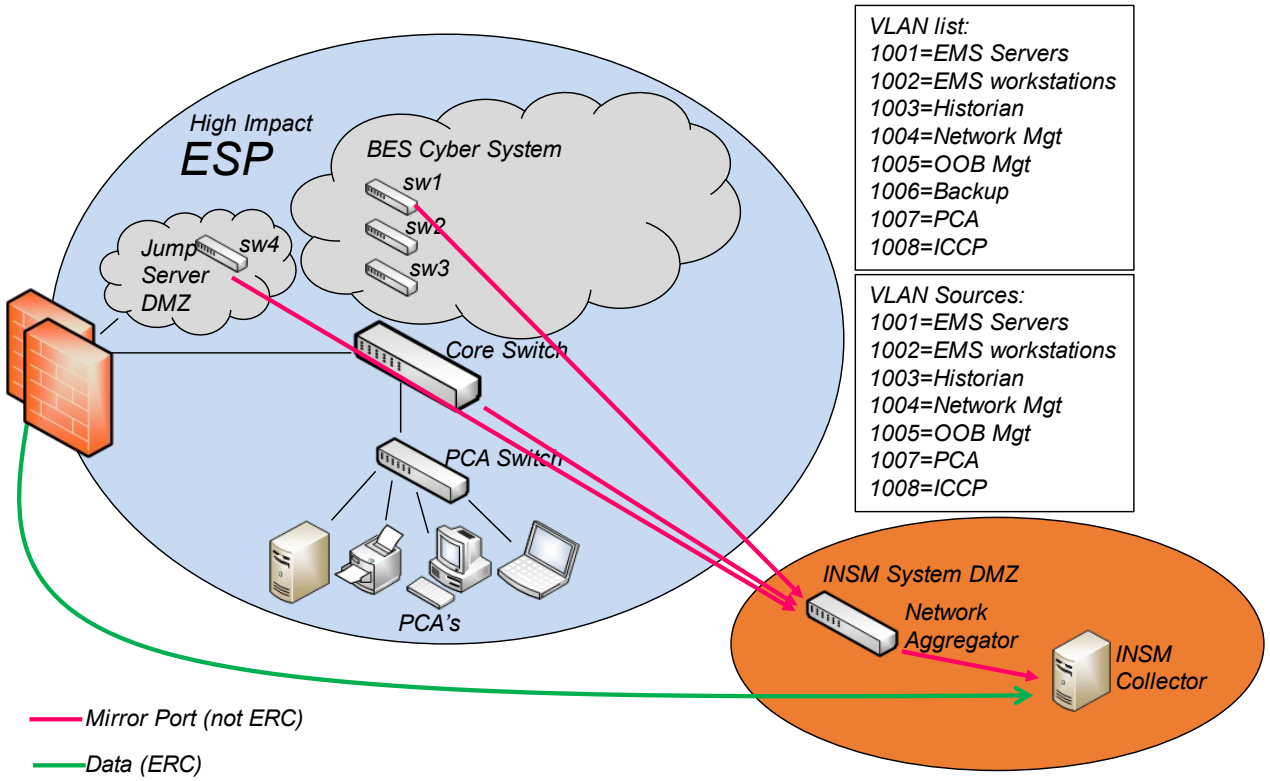

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FAQ for Reliability Standard CIP-015-1

April 5, 2024

CIP-015 – Cyber Security – Internal Network Security Monitoring

Q – What is internal network security monitoring (INSM)?

INSM refers to a forensic cyber security technology where entities copy network traffic in a trusted network zone, like an Electronic Security Perimeter (ESP), and redirect that copied network data to an INSM system that is capable of establishing a pattern of expected network traffic. FERC calls this pattern of expected network traffic a "baseline" in Order No. 887.[1] Once the expected network traffic baseline has been established, subsequent incoming network traffic is compared against the baseline and traffic that does not match the baseline in the INSM system is detected as anomalous and alerted on. These detections require analysis to determine if the anomalous network traffic is normal and benign, abnormal but not suspicious, or potentially malicious. FERC Order No. 887 states that, "INSM consists of three basic phases: (1) collection; (2) detection; and (3) analysis.[2] Taken together, these three stages provide the benefit for early detection and alerting of intrusions and malicious activity."[3]

Q – How is INSM different from traditional intrusion detection systems (IDS)?

Traditional IDS systems are categorized as performing signature-based detection of malicious activities. Similar to traditional anti-virus systems, IDS relies on an understanding of known malicious computer code for detection of malicious activity in a network. Duplicated network traffic sent to an IDS is then compared directly against the known signatures of malicious code implemented in the IDS. If the network traffic matches one of the signatures, an alert is issued. INSM does not typically use signatures of known malicious code. Instead, INSM relies on developing a pattern of expected network traffic and then compares incoming traffic against that pattern to identify potentially malicious traffic.

Additionally, IDS systems do not typically store the network traffic fed to them for further analysis. Network traffic data is usually discarded once the signature comparison takes place. On the other hand, INSM systems are typically capable of storing the network traffic and other metadata associated with the anomalous detection for further analysis and threat hunting while deleting non-anomalous network traffic to reduce storage requirements.

---

[1] ***Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems***, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 at P 9.

[3] *Id.* (citing Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2020/applied-collection-framework).

Q – What are the benefits of installing an INSM system?

FERC Order No. 887 paragraphs 10-12 describe the benefits as follow:

> *"The benefits of INSM can be understood by first describing the way attackers commonly compromise targets. Attackers typically follow a systematic process of planning and execution to increase the likelihood of a successful compromise. This process includes reconnaissance (e.g., information gathering), choice of attack type and method of delivery (e.g., malware delivered through a phishing campaign), taking control of the entity's systems, and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information). Thus, successful cyberattacks require the attacker to: (1) gain access to a target system; and (2) execute commands while in that system.*
>
> *INSM could better position an entity to detect malicious activity that has circumvented perimeter controls and gained access to the target system. Because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity of the attack and improve the entity's ability to stop the attack at its early phases.*
>
> *By providing visibility of network traffic that may only traverse internally within a trust zone, INSM can warn entities of an attack in progress. For example, properly placed, configured, and tuned INSM capabilities such as intrusion detection system and intrusion prevention system sensors could detect and/or block malicious activity early and alert an entity of the compromise. INSM can also be used to record network traffic for analysis, providing a baseline that an entity can use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal expected network activity and determine whether observed anomalous activity warrants further investigation. The recorded network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious activity."*[4]

[4] *Id.* PP 10-12.

Q – Why did the Drafting Team (DT) choose not to create a NERC Glossary of Terms for "anomalous"?

The DT considered whether or not to create a NERC Glossary of Terms entry for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT determined "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary of Terms.

> "Anomalous - adjective
>
> 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
> Example – Researchers could not explain the anomalous test results.
>
> 2 a: of uncertain nature or classification
>
> b: marked by incongruity or contradiction: PARADOXICAL[2]

Network anomaly detection is a well-known cyber security technique that provides network security threat detection. These systems track critical network characteristics in Real-time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Examples of such characteristics include excessive traffic volume, excessive bandwidth usage, or unusual protocol use. The DT determined that this technology has existed for many years, and it was unnecessary to define the term for industry. Many electric industry entities have already implemented, or are in the process of implementing, network anomaly detection solutions at their facilities. An additional reason for not defining the term is that "anomaly detection" is a phrase used by vendors to describe their proprietary technologies. However, in general, all vendors in the anomaly detection space compare incoming traffic against a baseline of known expected and normal traffic to detect something that is out of the ordinary, unusual, or unexpected. In a word: anomalous.

Q – Is network traffic required to be captured for Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs)?

The DT focused proposed Reliability Standard CIP-015-1, Requirement 1, on networks protected by an ESP. EACMS and PACS not protected by an entity's defined ESP are outside the scope of Project 2023-03 INSM. One example of EACMS and PACS Cyber Assets that are out of scope of Project 2023-03 INSM would be those existing in a demilitarized zone (DMZ) not protected by the entity's BES Cyber System's ESP(s).

Entities that choose to protect EACMS, PACS, and PCAs with a defined ESP should consider network traffic from those systems to be in scope for proposed Reliability Standard CIP-015-1, Requirement R1. Protected ESP networks connected to EACMS, PACS, and PCAs should be considered for data collection and monitoring for anomalous network traffic, as these systems are not immune from attempts to compromise, and they could serve as pivot points for an attack on a Bulk Electric System (BES) Cyber System protected by the same ESP.

[2] https://www.merriam-webster.com/dictionary/anomalous

Q – What does the DT mean by "network activity"?

In Order No. 887, FERC directed NERC to develop standards to address the need for Responsible Entities to monitor for and detect unauthorized activity, connections, devices, and software. The DT intends for the term "network activity" to represent the connections between devices and software included in the network traffic that an entity is collecting as it passes between hosts that are protected by an ESP.

Q – How should an entity decide which ESP networks to monitor and set up data feeds?

Entities are expected to identify which networks are protected by an ESP and use a risk-based rationale to determine where data feeds should be implemented to provide the best opportunities for detection of malicious activity, as set forth in proposed Reliability Standard CIP-015-1, Requirement R1, Part R1.1. Entities should document their risk-based rationale for assessing which networks to monitor in their INSM process.

For example, entities may choose not to collect data from networks that only carry backup traffic because workstations and servers do not typically route their normal traffic across that backup network. Otherwise, an entity would likely have to capture and temporarily store tremendous amounts of non-malicious backup traffic. From a risk-based perspective, backup networks pose limited risk and would likely not be a good use case for INSM. Likewise, monitoring of encrypted connections provides limited INSM value because all of the traffic passing on that network connection is encrypted, and INSM would be unable to decrypt and analyze the encrypted packets. An entity will realize more cyber security value, from an INSM perspective, if they monitor the decrypted traffic on the other ports on that switch where the VPN tunnel is connected. Entities need to document these kinds of evaluations of an entity's network as evidence for proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1.

A few examples of high-risk networks that should be given extra consideration for providing data feeds would include network traffic associated with an entity's energy management system (EMS) or distributed control system (DCS) server(s) and workstations, third-party connections, traffic associated with authentication servers (e.g., Active Directory or two-actor authentication systems, and programmable logic controller (PLC)/remote terminal units (RTU) communication paths). Each entity's ESP networks will be unique to that entity; therefore, the DT has left it up to the entity to make risk-based decisions, like those described, to determine what network traffic data feeds should be collected to provide the entity's INSM system with the best opportunity for detecting malicious traffic that could be indicative of an attack in progress.

Q – What is the difference between monitoring in CIP-005-7, CIP-007-6, and CIP-015-1?

Reliability Standard CIP-005-7 is exclusively concerned with the monitoring of ESPs. Reliability Standard CIP-005-7, Requirement R1, Part 1.5 requires entities to monitor at the ESP's Electronic Access Point, "For detecting known or suspected malicious communications for inbound and outbound communications." By specifying "known or suspected malicious traffic," it implies the use of signature-based detection methods for known malicious code. Requirement R1, Part 1.5 does not require monitoring of any traffic that is only passing between Cyber Assets within a defined ESP and is focused on traffic passing through the EAP.

FERC Order No. 887 aims to address this gap in cyber security monitoring by requiring INSM implementation.

Reliability Standard CIP-007-6, Requirement R3, Part 3.1 is focused on implementation of traditional signature-based technologies, such as anti-virus, on Cyber Assets. As noted above, this lack of a requirement for monitoring network traffic in the ESP represents a gap, as entities previously were not required to inspect internal ESP traffic for malicious activity.

While Reliability Standard CIP-007-6, Requirement 4, does allow logging of events at the BES Cyber System level, the DT would contend that most entities are meeting this requirement by logging events at the Cyber Asset level in a security information and event management (SIEM) system. The SIEM may also be used for analysis and retention of those host level events to meet Reliability Standard CIP-007-6, Requirement R4, and allow for detection of login attempts and malicious code on those Cyber Assets themselves. INSM would likely be unable to determine whether a login attempt failed or definitively detect malicious code installed on a Cyber Asset and is not a suitable technology to meet Reliability Standard CIP-007-6, Requirement R4, Part 4.1.

Proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1. will require entities to implement the method(s) of their choice to copy the network traffic the entity identified for capture in a defined ESP to a system that can identify patterns of expected network behavior. For proposed Requirement R1 Part 1.2, the INSM detects network traffic from the data feeds that is anomalous based on a comparison with the INSM system's patterns of expected network behavior. Network data associated with an anomalous detection should be protected and retained at least until the required evaluation can be completed in proposed Requirement R1, Part 1.3. The detection should be evaluated and triaged appropriately in proposed Requirement R1, Part 1.3. The DT considers proposed Reliability Standard CIP-015-1 to be an additional cyber security control that can increase the probability of detecting malicious activity in networks protected by an ESP.

Q – What data are entities required to retain and for how long?

Proposed Requirement R3 requires an INSM system to be able to store network traffic data and other metadata associated with each detection of anomalous activity. Data associated with non-anomalous traffic is not required to be retained. Most modern INSM systems are capable of saving just the data associated with anomalous network activity and discarding the rest.

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed by the entity not to be malicious do not need to be further retained after they have been evaluated in proposed Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's Reliability Standard CIP-008 incident response process(es) for further investigation. **Note:** Reliability Standard CIP-008 has its own retention requirements that entities need to keep in mind as they develop their proposed Reliability Standard CIP-015-1 retention process(es).

Q – How does the DT intend for entities to protect INSM data?

FERC Order No. 887 directed NERC to implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. In DT discussions it was clear that the intent was to protect the anomalous network data collected from being tampered with or removed by an adversary such that an entity could not accurately complete the required evaluation in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Malicious actors typically attempt to hide their tracks by removing evidence on a host system. Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.

Entities must protect their INSM data from unauthorized deletion or modification in support of proposed Requirements R1 and R3. Typically, this is done through the use of cyber and physical security controls. Entities should restrict electronic access to the INSM system and INSM data to only those with a need to access it. Restricting physical access to the INSM system is another good control. Use network segmentation to ensure that the INSM system is not part of the same networks the INSM system is monitoring. File integrity monitoring is another option to consider. Entities have developed a range of controls, and the controls they implement should be in line with their existing information protection programs.

Entities will need to assess the data being collected, and the meta data created by an INSM system, to determine if it needs to be protected as BES Cyber System Information (BCSI). Entities that declare the information stored in their INSM system as BCSI and protect the INSM data with their BCSI information protection procedures developed for Reliability Standard CIP-011-2, should meet proposed Reliability Standard CIP-015-1, Requirement R2. If an entity decides that the information is not BCSI, they must apply and document the security protections employed to protect the INSM data from modification or deletion.

Q – Why did the DT not include language that would allow a Technical Feasibility Exception (TFE) in situations where an entity believes they cannot implement INSM?

The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity's ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years.

Q – Is CIP-015-1 cost-effective?

In consideration of the cost effectiveness of proposed Reliability Standard CIP-015-1, the DT provided flexibility to entities to design their INSM systems to meet the proposed Reliability Standard CIP-015-1 requirements no matter the configuration of the individual networks protected by ESPs. Modern control center/data center environments should be capable of replicating an ESP's network traffic. Virtualized

systems should have the capability to replicate internal traffic between Virtual Cyber Assets to an INSM system. Replacing a switch or substation network device to replicate network traffic at key network convergence points is typically an inconsequential expense for an entity. The DT concluded that the main expense will most likely be procurement of INSM software and/or hardware, installation, labor count and cost, and tuning the system prior to the proposed Reliability Standard CIP-015-1 enforcement date.

The DT provided an implementation timeframe of 36 months for high impact and medium impact with External Routable Connectivity (ERC) control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those substation locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cyber security Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Q – Do entities have to capture traffic for serial connections?

As stated in the Technical Rationale, proposed Requirement R1 does not require collection of data such as serial communications, 4-20 ma circuits, or wide area network circuits such as multiprotocol label switching (MPLS) and other similar technologies.

[3] *Incentives for Advanced Cyber security Investment,* Order No. 893, 183 FERC ¶ 61,033, *order on reh'g,* Order No 893-A*,* 184 FERC ¶ 61.053 (2023); *see* e.g., FERC Cyber security Incentives web page - https://www.ferc.gov/cybersecurity-incentives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through April 17, 2024

Now Available

A formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Wednesday, April 17, 2024** for the following standard and implementation plan:

- CIP-015-1 – Internal Network Security Monitoring
  * Requirement R1 was updated to correct an error in the language from "BES Security Systems" to "BES Cyber Systems" to align with the clean version of Draft 2 of CIP-015-1.
- Implementation Plan

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships
Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

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 standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 12-17, 2024.**

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | Draft 2 of CIP-015-1
Comment Period Start Date:	4/5/2024
Comment Period End Date:	4/17/2024
Associated Ballots:	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 AB 2 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 Non-Binding Poll AB 2 NB Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan AB 2 OT

There were 55 sets of responses, including comments from approximately 142 different people from approximately 87 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

5. Please provide any additional comments for the DT 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
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Jay Sethi	Jay Sethi		MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO
					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
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
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities	4	WECC

						(Tacoma, WA)		
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Ryan Strom	Buckeye Power, Inc.	4	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Colette Caudill	East Kentucky Power Cooperative	1	SERC
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE

					Katrina Lyons	Georgia System Operations Corporation	4	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Bill Pezalla	Old Dominion Electric Cooperative	3,4	SERC
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE
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
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability	2	Texas RE

						Council of Texas, Inc.		
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC

Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC
Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State Department of Public Service	6	NPCC
David Kiguel	Independent	7	NPCC
Joel Charlebois	AESI	7	NPCC
Joshua London	Eversource Energy	1	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC
Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC

					Joel Charlebois	AESI	7	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
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
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

No additional comment.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE agrees with EEI comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

We support EEI's comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.

Likes 0	

Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports adding Generator Owner to the Applicability Section of the proposed CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this questions in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 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	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
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 RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
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 Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
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	

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments:

"We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.
Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.
Please clarify the term BES Security systems."

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc., so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

SRP disagrees with the proposed revision to Requirement R1 as it still has no guidance as to if detection is to be continuous or periodic. In addition, there is still no timeline as to how often detection and evaluation are to be performed. What if the technology is not available, and a RE wants to do this manually? Can the RE say they checked a tool once a year, such as wireshark, at a planned interval and call it compliant?

SRP is still unclear on what an auditor would look for evidence to meet this requirement. Would system logs, alert screens, email generated alerts, or others be acceptable evidence? Also, there needs to be guidance or a definition of a network communication baseline. This has yet been defined. The technical guidelines, provides an example of a baseline. However, the methods still do not call out what a baseline consists of. This needs to be included in the Methods of examples of what may be included in a baseline.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES believes using the phrase “Implement, using a risk-based rationale” without establishing minimal criteria could create a modification to the standard before it becomes effective. FERC has not approved of the ERO’s risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective.

Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1.

As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic, thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment
R1, Part 1.1: SPP respectfully asks the SDT to consider a “per system capability” clause due to potential technology limitations for entities (future technologies). **R1, Part 1.3:** Since Part 1.3 requires two separate actions, SPP recommends the following edit to the proposed language in R1, Part 1.3 (I.e., “change the word “to” to “and”): Implement one or more method(s) to evaluate activity detected in Part 1.2 and determine appropriate action.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	No
Document Name	

Comment
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

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 RSC	
Answer	No
Document Name	
Comment	

We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Please clarify the term BES Security systems.

Likes 0	
Dislikes 0	
Response	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	

We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Please clarify the term BES Security systems.

Likes 0	
Dislikes 0	
Response	

Ben Hammer - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	

The standards drafting committee needs develop NERC defined terms and definitions for the following terms:

- Anomalous Network activity

- Network Data Feeds

The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both.

The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

R1

The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that requirement R1, unlike requirements R2 and R3, does not include language such as, or is similar to, *"except during CIP Exceptional Circumstances"*. The Technical Rationale includes a discussion on "*Aligning Collection and Monitoring with Operations"* (p. 8) where it describes situations where *"Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Part 1.2. or 1.3."* While the SRC agrees with the Technical Rationale, the Technical Rationale is not enforceable. The SRC suggests that language such as, or similar to, the following be included within the requirement to establish clarity and encourage consistency in auditing practices:

Except during CIP Exceptional Circumstances or when Operational changes might require temporary or extended removal of INSM collection capability at specific locations.

R1.1

The SRC recommends that the standard be revised to clarify the intended meaning of "*risk-based rationale."* While the concept of "rationale" is well understood, it may be beneficial to create a sub-requirement (such as 1.1.1) where the term risk-based is clearly defined in such a way that encourages consistent audit practices. For example, in FAC-003-5 Transmission Vegetation Management, the Background section includes the following to describe the concept of risk-based:

"Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?"

The SRC is also concerned that the term "feed(s)" is not clear and could be misconstrued to not require collection of data. The SRC suggests that the term "feed(s)" be replaced with the term "collection point(s)". The SRC recommends the following revision:

1.1. Implement, using a risk-based rationale, network data collection points to monitor network activity; including connections, devices, and network communications.

The related language in M1 Part 1.1 should also be revised to reflect this change.

R1.2

The SRC proposes that the phrase “network data feed(s)” be replaced with “network data collection point(s)” to ensure consistency with R1.1 as indicated in the previous comment. The SRC recommends the following revision:

1.2. Implement one or more method(s) to detect anomalous network activity using the network data collection point(s) from Part 1.1.

M1

The SRC is concerned that M1 includes the language “Evidence must include”. This is inconsistent with most, if not all, of the NERC CIP standards and specifically with M2 and M3 of this standard, which state “Evidence may include”. The SRC recommends that the language in M1 be revised to be consistent with M2 and M3.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza

Answer	No
Document Name	

Comment

We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Please clarify the term BES Security systems.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that requiring entities to use a "risk-based rationale" to designing and implementing INSM is (a) unnecessary - an entity either has or hasn't implemented INSM in a manner that covers all BES Cyber Systems within an ESP, and (b) could result in endless arguments among Responsible Entities, Regions, and NERC over what might be considered acceptable approaches to establishing a risk-based rationale for implementation choices.

NST suggests not using the phrase, "network data feeds," as the term, "data feeds" is widely used to describe data made available to users, typically via web servers, that provides real-time information about road conditions, weather, stock indices, etc.

NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection methods and locations, which may be either physical or virtual, used to monitor network activity including connections, devices, and network communications."

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan

Answer	No
Document Name	

Comment

Is this risk is based on reliability only or other things as well? More details need to be provided.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Likes 0	
Dislikes 0	

Response

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer	No
Document Name	

Comment

SMECO agrees with ACES comments:

ACES believes using the phrase “Implement, using a risk-based rationale” without establishing minimal {C}[A1]{C} criteria could create a modification to the standard before it actually becomes effective. FERC has not approved of the ERO’s risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective.

Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1.

As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic, thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD appreciates the efforts of the Standards Drafting Team (SDT) in responding to the industry's comments on the initial draft and proposing these new revisions so quickly. In Requirement R1 Part 1.1, instead of using the words "network data feeds" we prefer the original wording of "data collection locations", or alternately "data collection sources" because the wording of "data collection feeds" could be interpreted as a *subscription* to threat/intelligence feeds.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2.

The use of the 'risk-based rationale' language in CIP-015 R1.1 is leaving it to the discretion of entities to determine which component poses higher or lower risks. This will leave it open to the auditor's interpretation and expectation instead of ensuring the scope is concise and clear under this requirement. BC Hydro recommends to define the parameters of these 'risks' to give clear direction to entities or specify the network components on which this Requirement R1.1 applies.

BC Hydro has concerns in relation to the use of term "anomalous activity" as this could be varied in terms of application and usage and is left to the entities to interpret. BC Hydro also concerns over the expected evidence needed for "documentation of responses to detected anomalies" per Measure M1 to meet Part R1.3., which seems to indicate that proof that all detections were responded to regardless whether they were false positives will be required, i.e. proving the negative on all anomalies detected. Due to this BC Hydro has concerns over a very high amount of data which needs to be

analyzed and documented based on Requirement R1 Part R1.3 as drafted. BC Hydro recommends to make the scope concise in the language of CIP-015 Requirement R1 Part R1.3, and add example scenarios and use-cases in the Technical Rationale.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

For R1.2, if the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes that adding the phrase “using a risk-based rationale” reduces but does not eliminate ambiguity about the requirement. Ambiguity opens REs to subjective criticism from auditors. Therefore, BPA still recommends adding language used elsewhere in the CIP Standards, specifically “as determined by the Registered Entity”, to strengthen the position that the REs are empowered to set their own risk-based rationale.

BPA supports discontinuing the term “locations” in R1. However, not every RE will refer to the two books cited in the Technical Rationale to develop an understanding of the newly proposed term “network data feed”. The Technical Rationale provides a lengthy, complex explanation of the intent of the term. BPA requests that the SDT include a brief, simple, clear definition in addition to the three paragraphs of explanation.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	2023-03 Unofficial_Comment_Form_April 2024 NSRF.docx
Comment	

MRO NSRF thanks the drafting team for an excellent job in addressing stakeholder comments and adjusting the standard language.

For R1, R2 and R3 we suggest beginning each with either “The” or “Each” to match CIP-002, CIP-012 and CIP-013.

The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:

The/Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:

Likes 0	
Dislikes 0	
Response	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Ameren agrees with and supports EEI and NAGF comments.

Likes 0	
Dislikes 0	
Response	

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for Question #2 regarding potential non-substantive changes the drafting team could make to R1, R2, and R3.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R1 and Measurement M1.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

Robert Follini - Avista - Avista Corporation - 3

Answer	Yes
Document Name	

Comment

Avista agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.

While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration:We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.

Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…":

"**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:"

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration: We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": "**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:"	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment
NEE agrees with EEI comments: EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration: We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": "**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. The documented process(es) **and** shall include each of the following requirement Parts:"

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment
Black Hills Corporation agrees with EEI comments: While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration: • We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. • Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": "**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (*remove: "to"*). **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. *(remove: "The documented process(es)")* **and** shall include each of the following requirement Parts:"

Likes 0	
Dislikes 0	

Response

Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The updated language to R1 implies that the Responsible Entity would be implementing data feeds into their environment to monitor network activity. The intent of this requirement is to identify which data feeds within the environment the Responsible Entity will be monitoring network activity. We would suggest removing “implement” and reinstating “identify”.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy requests that the Regulating Body has determined an INSM as applicable to CIP-015. Until this is clear, there could be various interpretations for compliance. Understanding this interpretation will be a challenge for all to come to a conclusion of a baseline and must come to a consensus based on individual interpretation.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing stakeholder comments and adjusting the standard language. For R1, R2 and R3 MH suggests beginning each with either “The” or “Each” to match CIP-002, CIP-012 and CIP-013. This is a non-substantive change. The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:	

The/Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. The documented process(es) shall provide methods for detecting and evaluating anomalous network activity and shall include each of the following requirement Parts:

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
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	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the SDT's consideration if previous comments submitted. In order to clarify and ensure the measures and requirement language are aligned, Texas RE recommends adding "documented" in front of risk-based rationale in Requirement Part 1.1: 1.1 Implement, using a *documented* risk-based rationale, network data feed(s)…	
Likes 0	
Dislikes 0	
Response	

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA recommends adjusting the wording of R2 to eliminate confusing grammar: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to mitigate the risks of unauthorized deletion or modification of internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3.”

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2.

It is not clear if the Requirement R2 is expecting both detection of unauthorized access and/or changes along with protection mechanisms to prevent unauthorized access or if the entity can choose what combination of controls is appropriate to them based on their security risk tolerance. BC Hydro recommends to provide clarity in the Requirement R2 to remove ambiguity and scope these accurately. BC Hydro also notes that although Technical Rationale provides examples of guidance it is not an ERO endorsed compliance guidance document. Auditors may chose to adhere to certain aspects from Technical Rationale and choose to leave others.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No

Document Name	
Comment	

SMUD recommends the Standards Drafting Team swap Requirements R2 and R3 to better align the requirements in the order they should be implemented.

Requirement R2 is to “protect” INSM data against unauthorized deletion in support of Requirement R3. Requirement R3 is to “retain” INSM data associated with network activity determined to be anomalous. The methods to “detect” anomalous network activity should be addressed *before* methods to “protect” INSM data against unauthorized deletion. Therefore, we recommend moving R2 to R3, and R3 to R2. We feel that this change would be non-substantive and could be made in the final ballot.

Likes 0	
Dislikes 0	
Response	

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer	No
Document Name	
Comment	

SMECO agrees with ACES comments:

While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used:

“….to mitigate the risks to the confidentiality, integrity, and availability of the collected data.”

Likes 0	
Dislikes 0	
Response	

Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan

Answer	No
Document Name	
Comment	

More clarity is required on which data needs to be protected. What is meant by protection method (mitigation of unauthorized modification)?

Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST recommends that R2 address the protection of collected INSM data both in storage and in transit (e.g., from a substation with medium impact BCS with ERC to a SIEM system located at an entity's headquarters or a Control Center).	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	
R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
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 RSC	
Answer	No
Document Name	
Comment	
R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used: “….to mitigate the risks to the confidentiality, integrity, and availability of the collected data.”	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection."	

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	Yes
Document Name	

Comment

The wording of requirement R2 and M2 clearly outline the requirements. A non-substantive change is suggested to re-order R2 and R3, so that a future requirement is not referenced. This will make it easier to read the standard in order. If this is adopted, then references to R3 would become R2.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

No additional comment.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI comments:

EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.

Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE agrees with EEI comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments.	

Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	

Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R2 and Measurement M2.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The wording of requirement R2 and M2 clearly outline the requirements. MRO NSRF suggests a non-substantive change to re-order Requirements (and consequently Measures) R2 and R3 so that this requirement refers back to requirements already read vs. both back and forward to a requirement not yet read, making the standard easier to understand when reading it in order. If adopted the reference to R3 would need to be changed to R2.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this questions in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Amy Wilke - American Transmission Company, LLC - 1

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

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments:

"We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations."

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

SRP disagrees with the proposed language in Requirement R3. For example, CIP-007 R4, states that logs are retained for 90 days. The current draft of CIP-015 does not state a time frame to keep logs. How long should REs keep evidence? Should each RE make this determination and possibly write up a policy on saving data for a time frame of their choosing? If that is the case, each RE will be able to keep a different amount of data, some more some less. Would that be acceptable to an auditor or is that the intent of the drafting team? SRP prefers language added in the requirement stating how each RE must store x days of data at minimum or that each RE must retain data to show compliance.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order.

Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

R3: SPP asks that the SDT provide additional clarity around what is a reasonable duration for data retention. The current language places the burden on the entity to determine that duration, but records retention for ERO compliance monitoring and enforcement could significantly lengthen how long an entity is required to retain the data and place a significant cost on an entity for storing that data. A more prescriptive time period (e.g., 90 days, 180 days) would seem reasonable to include in the R3 requirement language, and precedence currently exists in the NERC CIP Standards for security event logging today (CIP-007-6, R4, Part 4.3).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dominion Energy is concerned about the use of the word "detailed" when describing the level of INSM data that should be retained. What information would be required to be retained that is not relevant to the anomalous activity if full packet capture data is not required?

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
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 RSC	
Answer	No
Document Name	
Comment	
We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	

Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	

AES supports MRO NSRF comments listed below

The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests **eliminating CIP-015 R3** and **adding a new sub part 1.4** a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
See response to question 1	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The SRC is concerned that the language “internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2” is not sufficiently clear and will lead to auditing challenges. The concept of “relevant to anomalous network activity” can be construed in many ways, and different auditors may come to different conclusions regarding the relevance of certain network activity. To ensure consistency with R1.2 and R1.3, the SRC recommends that the determination of what is “*anomalous”* be left to those sub-requirements and the term *“relevant to”* be replaced with the term “related to”. The SRC recommends the following note language revision: Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not related to network activity detected and evaluated under Requirement R1, Parts 1.2 and 1.3. It is also unclear what action the phrase “until the action is complete” is intended to refer to, and the SRC recommends that this be clarified.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	

We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan

Answer	No
Document Name	

Comment

We would prefer to have a defined timeframe for data retention similar to CIP-007 Requirement R4.

Likes 0	
Dislikes 0	

Response

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer	No
Document Name	

Comment

SMECO agrees with ACES comments: Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order.Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
BPA appreciates the clarification in R3 and the Technical Rationale regarding which data must be retained. However, we note that there is potential for voluminous data to be flagged as “anomalous”, especially during the time it will take to tune the process. BPA does not support the retention timeframe “until the action is complete.” It is unclear if this phrase is referring to the evaluation required by Part 1.3, the determination of further actions required by Part 1.3, or the “further actions” mentioned in Part 1.3. BPA notes that the latter could include risk mitigation or recovery actions that span a considerable length of time.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	

Comment
Exelon is responding to this question in alignment with the EEI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment
Exelon is responding to this questions in alignment with the EEI.

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. SIGE also appreciates the note at the end of the requirement, as it helps add clarity.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. CEHE also appreciates the note at the end of the requirement, as it helps add clarity.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R3 and Measurement M3.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Avista agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	Yes
Document Name	

Comment

ITC supports EEI’s comments.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

We support EEI's comments:

EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	Yes
Document Name	

Comment

The wording of the Note under Requirement R3 can be improved by revising it to state “(for example, full packet capture data, etc.)”, or alternately “(e.g. full packet capture data, etc.)”. As the Note is currently written, an entity may assume that “full packet capture” is a *requirement* for internal network security monitoring in Requirement R1, whereas the intent of the Note seems to be to provide an example of the data that is not required to be obtained. This change would be non-substantive and could be made in the final ballot.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE agrees with EEI comment: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Only retaining the data that is associated with network activity determined to be anomalous could lead to a forensics issue if the traffic is within the current baseline and not pre-identified as an anomaly. With the current language of the standard this data would not be retained. Responsible Entities should reevaluate the “normal” traffic baseline on a periodic basis to ensure that they are identifying any anomalous activity to address this risk.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	

Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro does not believe the note is necessary but does not object to adding the note if it promotes consensus. Manitoba Hydro suggests that the word “detailed” and parenthetical example be removed to clarify and preserve the intent of the note. [Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.]	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Who gets to or how is it determined what data is not relevant? What if an entity doen't think it was relevant but an auditor does?	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
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	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE understands the phrase “until the action is complete” to mean that if further action is determined to be necessary in accordance with Requirement Part 1.3, the data shall be retained until that further action is completed. Texas RE agrees with retaining network activity determined to be anomalous until the action is completed, except for anomalous activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident. For anomalous network activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident Texas RE recommends setting the retention period to one calendar year after the completion of the action.	
Likes 0	
Dislikes 0	
Response	

5. Please provide any additional comments for the DT to consider, if desired.

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	
Document Name	

Comment

FirstEnergy supports EEI Comments which state:

EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	
Dislikes 0	

Response

Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	
Document Name	

Comment

The Technical Rationale document can use additional editing to align with the edited standards. For example. On Page 6 near the bottom there is a section titled “Data Collection Locations” that in the first sentence redlines out “collection locations” in favor of “feed(s)” which aligns with the standard. Yet the section title continues to focus on “Locations” as well as the content within the section, even though the standard is now related to “feed(s)”.

Likes 0	
Dislikes 0	

Response

Tyler Schwendiman - ReliabilityFirst - 10

Answer	
Document Name	

Comment

The Drafting Team should consider requirement language pertaining to the testing of their program put in place to detect anomalous activity on the Responsible Entity’s network to ensure their controls are working properly. The Drafting Team should also consider requirement language pertaining to the ability to detect instances where the protections put in place are not working properly to reduce the response time of the program not functioning as intended similar to CIP-007-6 R4 P4.2.2.

Likes 0	
Dislikes 0	

Response

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment
Displaying the requirement, parts and subparts in the table format with the "Applicable Systems, Requirements, and Measures," is the preferred formatting.

Likes 0	
Dislikes 0	

Response

Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez

Answer	
Document Name	

Comment
We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	
Document Name	

Comment
Black Hills Corporation agrees with EEI comments: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	

NEE agrees with EEI comment: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	
Document Name	
Comment	

We support EEI's comments:

EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	

Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	
ITC supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide. Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a	

Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
The NAGF has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST disagrees with the SDT's decision to demote network baselining from a Requirement to a Measure, which is essentially nothing more than a suggestion, for two reasons:	

> FERC Order 887 Paragraph 5 states explicitly, "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment."

> We are hard-pressed to imagine how anyone using INSM could detect anomalous network behavior without a baseline. To that point, Order 887 Paragraph 12 states, "Establishing baseline network traffic allows entities to define what is and is not normal and expected network activity and determine whether observed anomalous activity warrants further investigation."

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	
Document Name	

Comment

Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for Question #5.

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment
Southern Company agrees with the additional comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	
Document Name	

Comment
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1,6	
Answer	
Document Name	

Comment
The standards drafting committee needs develop NERC defined terms and definitions for the following terms: • Anomalous Network activity • Network Data Feeds The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both. The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between 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 RSC	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	
Document Name	
Comment	

CEHE would like to restate that CEHE does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. CEHE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

CEHE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.

Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	
Comment	

SIGE would like to restate that SIGE does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

SIGE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.

Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1

Answer	
Document Name	
Comment	

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**

Likes 0	
Dislikes 0	
Response	

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	
Comment	

Implementation Plan: Entities will require sufficient time to research and identify new technology solutions to meet the new INSM requirements. Implementation could require significant changes and/or additions to existing network architectures. Therefore, SPP appreciates and endorses the 36-month timeframe for implementation.

Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	
Document Name	
Comment	

ACES believes the proposed requirements of CIP-015-1 are out of order and should be re-numbered. As currently written, Requirement R2 references Requirements R1 and R3; therefore, ACES believes it should be placed after the current Requirements R1 and R3.

ACES would like to thank the SDT for its hard work.

Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
SRP recommends having baseline defined in the Measures rather than in the technical guidance.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements."	
Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2023-03 Internal Network Security Monitoring | Draft 2 of CIP-015-1
Comment Period Start Date:	4/5/2024
Comment Period End Date:	4/17/2024
Associated Ballot(s):	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 AB 2 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 Non-Binding Poll AB 2 NB 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan AB 2 OT

There were 55 sets of responses, including comments from approximately 142 different people from approximately 87 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, Soo Jin Kim (via email) or at (404) 446-9742.

Questions

****Please Note: Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

  Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.
- **R3 (previously R2):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*
- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT received supportive comments for adding the Generator Owner to 4.1.4. of the Applicability Section.

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

For Requirements R1, R2 and R3, the DT added the word "Each" at the beginning of the requirements to align with the CIP family of standards.

The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. Using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. In addition, the DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)."

Each entity is expected to develop an INSM system that continuously compares incoming traffic to its established baseline of expected network traffic to detect anomalous network activity. However, the drafting team envisioned scenarios where an entity would want to pause monitoring for a period of time (during equipment maintenance or replacement) or INSM equipment could fail, and continuous

monitoring be interrupted. The DT did not want entities to be subject to a potential finding of non-compliance during these scenarios and thus did not specify continuous monitoring in the requirements.

The DT considered whether or not to create a NERC Glossary term for "anomalous". The Merriam-Webster dictionary defined anomalous as:

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction: PARADOXICAL

The DT addresses this in the FAQ document, and has provided some updates to the Technical Rationale document for additional clarity.

The DT did not add CIP Exceptional Circumstance to Requirement R1 because it was determined that once an entity has established and documented their process and methods for performing INSM in their ESP networks, a CIP Exceptional Circumstance should not materially impact their INSM program from the perspective that the equipment would already be installed, and a detection and evaluation process has already been implemented. While continuous monitoring is the goal of the standard, the DT did not include a continuous monitoring requirement to allow for situations where an entity has an equipment failure, needs to perform maintenance that would interrupt monitoring, or determines that the INSM system should be shut down for a period of time to perform generation plant or substation maintenance. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including "risk-based rationale" is more encompassing than alternative language proposed by several commenters.

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

***Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

  Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

- **R3 (previously R2):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

The intent of Requirement R3 (previously R2) is to protect the collected INSM data from modification or deletion by an adversary. The Technical Rationale has been updated to read: "The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary.

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

***Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the actual changes in the requirements and measure from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

  Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

- **R3 (previously R2):** Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data

retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged.

In response to commenters, the DT updated the Note in Requirement R2 (previous Requirement R3) to "Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2," to clarify the intent of the Note. The word "detailed" was removed, as information would not be required to be retained that is not relevant to the anomalous activity.

5. Please provide any additional comments for the DT to consider, if desired.

Summary Response:

Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged.

The Technical Rationale has been updated to read: ~~The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[1]"~~ The Responsible Entity's existing process(es) should be

referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.

The DT considered whether or not to create a NERC Glossary term for "anomalous." The Merriam-Webster dictionary defined anomalous as:

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction: PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity.

The INSM system may be classified as BCSI or EACMS per the existing processes for each entity.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 are outside of the scope of Project 2023-03.

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations, which may be more challenging to implement.

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
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	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Jay Sethi	Jay Sethi		MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO

					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
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
					John Nierenberg	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
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company -	1	SERC

						Southern Company Services, Inc.		
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Ryan Strom	Buckeye Power, Inc.	4	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Colette Caudill	East Kentucky Power Cooperative	1	SERC
					Tony Kroskey	Brazos Electric Power	1	Texas RE

						Cooperative, Inc.		
					Katrina Lyons	Georgia System Operations Corporation	4	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Bill Pezalla	Old Dominion Electric Cooperative	3,4	SERC
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE
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

					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6			Micah Runner	Black Hills Corporation	1	WECC

				Black Hills Corporation - All Segments	Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated	1	NPCC

	Edison Co. of New York		
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State Department of Public Service	6	NPCC
David Kiguel	Independent	7	NPCC
Joel Charlebois	AESI	7	NPCC
Joshua London	Eversource Energy	1	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC

					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Joel Charlebois	AESI	7	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
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
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE agrees with EEI comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI’s comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports adding Generator Owner to the Applicability Section of the proposed CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's and NAGF's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this questions in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
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 RSC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc., so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
SRP disagrees with the proposed revision to Requirement R1 as it still has no guidance as to if detection is to be continuous or periodic. In addition, there is still no timeline as to how often detection and evaluation are to be performed. What if the technology is not available, and a RE wants to do this manually? Can the RE say they checked a tool once a year, such as wireshark, at a planned interval and call it compliant? SRP is still unclear on what an auditor would look for evidence to meet this requirement. Would system logs, alert screens, email generated alerts, or others be acceptable evidence? Also, there needs to be guidance or a definition of a network communication baseline. This has yet been defined. The technical guidelines, provides an example of a baseline. However, the methods still do not call out what a baseline consists of. This needs to be included in the Methods of examples of what may be included in a baseline.	
Likes 0	

Dislikes 0	

Response

Thank you for your comments. Each entity is expected to develop an INSM system that continuously compares incoming traffic to its established baseline of expected network traffic to detect anomalous network activity. However, the drafting team envisioned scenarios where an entity would want to pause monitoring for a period of time (during equipment maintenance or replacement) or INSM equipment could fail and continuous monitoring be interrupted. The DT did not want entities to be subject to a potential finding of non-compliance during these scenarios and thus did not specify continuous monitoring in the requirements. The scenario you suggest would not be an acceptable method to meet the requirements, however. Depending on the INSM tools the entity selects, the baseline could be created using different vendor proprietary methods. Given that there is not a single method of developing a baseline that could apply to all vendor products and future INSM solutions using new tools such as AI, the DT chose not to provide specifics in Requirement R1 for how to develop a baseline. Section C of the standard provides information on evidence retention.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES believes using the phrase “Implement, using a risk-based rationale” without establishing minimal criteria could create a modification to the standard before it becomes effective. FERC has not approved of the ERO’s risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective.

Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1.

As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic,

thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.	
Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.

The DT notes that many encrypted protocols (including HTTPS) are not fully encrypted, which allows INSM systems to monitor important information, such as certificates and user-agent strings. We note that collecting this data allows entities to detect and alert on several attack techniques even for protocols with bolted on transport layer security encryption. Last, many SCADA systems require the use of active directory or similar directories, server message block and similar file transfer systems which encrypt portions of payloads, but not all of the payload. An INSM system can carve files from these protocols, including active directory group policy settings.

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

R1, Part 1.1: SPP respectfully asks the SDT to consider a "per system capability" clause due to potential technology limitations for entities (future technologies).

R1, Part 1.3: Since Part 1.3 requires two separate actions, SPP recommends the following edit to the proposed language in R1, Part 1.3 (I.e., "change the word "to" to "and"):

Implement one or more method(s) to evaluate activity detected in Part 1.2 and determine appropriate action.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity's ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years. The DT disagreed with your suggestion to change "to" to "and," as doing so would create a requirement for two activities. The DT intended the evaluation to lead entities to a conclusion on what action they should take. Those actions could be determining the anomalous network traffic is a legitimate and benign false positive, is abnormal but not malicious perhaps requiring a configuration change, or potentially malicious and needs to be escalated to your CIP-008 process for handling as a possible cybersecurity incident or attempt to compromise.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ISO/RTO IRC’s comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems.	
Likes 0	

Dislikes 0	

Response

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. Using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. In addition, the DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)."

"BES Security Systems" was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be "BES Cyber Systems." This was reflected correctly in the clean version of the document.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Please clarify the term BES Security systems.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. "BES Security Systems" was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be "BES Cyber Systems." This was reflected correctly in the clean version of the document.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
The standards drafting committee needs develop NERC defined terms and definitions for the following terms: • Anomalous Network activity • Network Data Feeds The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both. The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for "anomalous". The Merriam-Webster dictionary defined anomalous as:	

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction: PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity.

The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 is outside of the scope of Project 2023-03.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	

R1

The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that requirement R1, unlike requirements R2 and R3, does not include language such as, or is similar to, *"except during CIP Exceptional Circumstances"*. The Technical Rationale includes a discussion on "*Aligning Collection and Monitoring with Operations"* (p. 8) where it describes situations where *"Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Part 1.2. or 1.3."* While the SRC agrees with the Technical Rationale, the Technical Rationale is not enforceable. The SRC suggests that language such as, or similar to, the following be included within the requirement to establish clarity and encourage consistency in auditing practices:

Except during CIP Exceptional Circumstances or when Operational changes might require temporary or extended removal of INSM collection capability at specific locations.

R1.1

The SRC recommends that the standard be revised to clarify the intended meaning of "*risk-based rationale*." While the concept of "rationale" is well understood, it may be beneficial to create a sub-requirement (such as 1.1.1) where the term risk-based is clearly defined in such a way that encourages consistent audit practices. For example, in FAC-003-5 Transmission Vegetation Management, the Background section includes the following to describe the concept of risk-based:

"Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?"

The SRC is also concerned that the term "feed(s)" is not clear and could be misconstrued to not require collection of data. The SRC suggests that the term "feed(s)" be replaced with the term "collection point(s)". The SRC recommends the following revision:

1.1. Implement, using a risk-based rationale, network data collection points to monitor network activity; including connections, devices, and network communications.

The related language in M1 Part 1.1 should also be revised to reflect this change.

R1.2

The SRC proposes that the phrase "network data feed(s)" be replaced with "network data collection point(s)" to ensure consistency with R1.1 as indicated in the previous comment. The SRC recommends the following revision:

1.2. Implement one or more method(s) to detect anomalous network activity using the network data collection point(s) from Part 1.1.

M1

The SRC is concerned that M1 includes the language “Evidence must include”. This is inconsistent with most, if not all, of the NERC CIP standards and specifically with M2 and M3 of this standard, which state “Evidence may include”. The SRC recommends that the language in M1 be revised to be consistent with M2 and M3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT did not add CIP Exceptional Circumstance to Requirement R1 because it was determined that once an entity has established and documented their process and methods for performing INSM in their ESP networks a CIP Exceptional Circumstance should not materially impact their INSM program from the perspective that the equipment would already be installed and a detection and evaluation process has already been implemented. While continuous monitoring is the goal of the standard, the DT did not include a continuous monitoring requirement to allow for situations where an entity has an equipment failure, needs to perform maintenance that would interrupt monitoring, or determines that the INSM system should be shut down for a period of time to perform generation plant or substation maintenance. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters. The DT received comments that referenced “locations” could be confused with geographic locations, so the DT modified “network data locations and methods” with “network data feed(s).” Using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	
We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.	

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system. “BES Security Systems” was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be “BES Cyber Systems.” This was reflected correctly in the clean version of the document.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that requiring entities to use a "risk-based rationale" to designing and implementing INSM is (a) unnecessary - an entity either has or hasn't implemented INSM in a manner that covers all BES Cyber Systems within an ESP, and (b) could result in endless arguments among Responsible Entities, Regions, and NERC over what might be considered acceptable approaches to establishing a risk-based rationale for implementation choices. NST suggests not using the phrase, "network data feeds," as the term, "data feeds" is widely used to describe data made available to users, typically via web servers, that provides real-time information about road conditions, weather, stock indices, etc.	

NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection methods and locations, which may be either physical or virtual, used to monitor network activity including connections, devices, and network communications."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale that can be leveraged to develop an INSM. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters. Numerous comments were received expressing support for providing flexibility to Responsible Entities to develop their programs without having specific timelines and obligations that may not align to the operations of all Responsible Entities. We provided details in the Technical Rationale that can be used to support the INSM programs for the Responsible Entities. Additionally, the DT updated the Technical Rationale with additional language to clarify the word “baseline” when used to describe anomaly detection technology. The DT reviewed your comment but decided Requirement R1, Part 1.1 is written as intended, so made no change.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	
Is this risk is based on reliability only or other things as well? More details need to be provided. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.	
Likes 0	

Dislikes 0	

Response
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale that can be leveraged to develop an INSM. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including "risk-based rationale" is more encompassing than alternative language proposed by several commenters. Numerous comments were received expressing support for providing flexibility to Responsible Entities to develop their programs without having specific timelines and obligations that may not align to the operations of all Responsible Entities. We provided details in the Technical Rationale that can be used to support the INSM programs for the Responsible Entities.

Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	

Comment
SMECO agrees with ACES comments: ACES believes using the phrase "Implement, using a risk-based rationale" without establishing minimal {C}[A1]{C} criteria could create a modification to the standard before it actually becomes effective. FERC has not approved of the ERO's risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective. Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1.

As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic, thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD appreciates the efforts of the Standards Drafting Team (SDT) in responding to the industry's comments on the initial draft and proposing these new revisions so quickly. In Requirement R1 Part 1.1, instead of using the words "network data feeds" we prefer the original wording of "data collection locations", or alternately "data collection sources" because the wording of "data collection feeds" could be interpreted as a *subscription* to threat/intelligence feeds.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)."	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2.

The use of the 'risk-based rationale' language in CIP-015 R1.1 is leaving it to the discretion of entities to determine which component poses higher or lower risks. This will leave it open to the auditor's interpretation and expectation instead of ensuring the scope is concise and clear under this requirement. BC Hydro recommends to define the parameters of these 'risks' to give clear direction to entities or specify the network components on which this Requirement R1.1 applies.

BC Hydro has concerns in relation to the use of term "anomalous activity" as this could be varied in terms of application and usage and is left to the entities to interpret. BC Hydro also concerns over the expected evidence needed for "documentation of responses to detected anomalies" per Measure M1 to meet Part R1.3., which seems to indicate that proof that all detections were responded to regardless whether they were false positives will be required, i.e. proving the negative on all anomalies detected. Due to this BC Hydro has concerns over a very high amount of data which needs to be analyzed and documented based on Requirement R1 Part R1.3 as drafted. BC Hydro recommends to make the scope concise in the language of CIP-015 Requirement R1 Part R1.3, and add example scenarios and use-cases in the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided

additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. The DT considered whether or not to create a NERC Glossary term for "anomalous". The Merriam-Webster dictionary defined anomalous as: Anomalous - adjective 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL Example - Researchers could not explain the anomalous test results. 2 a: of uncertain nature or classification b: marked by incongruity or contradiction: PARADOXICAL The DT created a FAQ document that addresses this, as well as updated the Technical Rationale document for additional clarity.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
For R1.2, if the term "anomalous" is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to "include criteria to evaluate and define attempts to compromise". If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding "anomalous" and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their "anomalous" criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous”. The Merriam-Webster dictionary defined anomalous as: Anomalous - adjective 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL Example - Researchers could not explain the anomalous test results. 2 a: of uncertain nature or classification b: marked by incongruity or contradiction: PARADOXICAL The DT created a FAQ document that addresses this, as well as updated the Technical Rationale document for additional clarity.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes that adding the phrase “using a risk-based rationale” reduces but does not eliminate ambiguity about the requirement. Ambiguity opens REs to subjective criticism from auditors. Therefore, BPA still recommends adding language used elsewhere in the CIP Standards, specifically “as determined by the Registered Entity”, to strengthen the position that the REs are empowered to set their own risk-based rationale. BPA supports discontinuing the term “locations” in R1. However, not every RE will refer to the two books cited in the Technical Rationale to develop an understanding of the newly proposed term “network data feed”. The Technical Rationale provides a lengthy, complex explanation of the intent of the term. BPA requests that the SDT include a brief, simple, clear definition in addition to the three paragraphs of explanation.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	2023-03 Unofficial_Comment_Form_April 2024 NSRF.docx
Comment	
MRO NSRF thanks the drafting team for an excellent job in addressing stakeholder comments and adjusting the standard language. For R1, R2 and R3 we suggest beginning each with either “The” or “Each” to match CIP-002, CIP-012 and CIP-013. The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”: **The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. For Requirements R1, R2, and R3, the DT added the word “Each” at the beginning of the requirements to align with the CIP family of standards. The suggested clarity revision was not made because the DT believes Requirement R1 is clear as written.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's and NAGF's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for Question #2 regarding potential non-substantive changes the drafting team could make to R1, R2, and R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R1 and Measurement M1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration:We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.	

Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": "**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:"	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. For Requirements R1, R2, and R3, the DT added the word "Each" at the beginning of the requirements to align with the CIP family of standards. The suggested clarity revision was not made because the DT believes Requirement R1 is clear as written.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment
We support EEI's comments: EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration: We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": "**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:"

Likes 0	
Dislikes 0	

Response
Thank you for your support. Please see responses to EEI's comments.

Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment
NEE agrees with EEI comments: EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration:

We suggest adding the word “The” or “Each” to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.

Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:

“**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. The documented process(es) **and** shall include each of the following requirement Parts:”

Likes 0	
Dislikes 0	

Response
Thank you for your support. Please see responses to EEI’s comments.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with EEI comments:

While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team’s consideration:

- We suggest adding the word “The” or “Each” to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.
- Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:

"**The/Each** Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (*remove: "to"*). **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. *(remove: "The documented process(es)")* **and** shall include each of the following requirement Parts:"	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The updated language to R1 implies that the Responsible Entity would be implementing data feeds into their environment to monitor network activity. The intent of this requirement is to identify which data feeds within the environment the Responsible Entity will be monitoring network activity. We would suggest removing "implement" and reinstating "identify".	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT previously used "identify" and commenters suggested that language was not clear, so the DT made the change to "implement."	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment
FirstEnergy requests that the Regulating Body has determined an INSM as applicable to CIP-015. Until this is clear, there could be various interpretations for compliance. Understanding this interpretation will be a challenge for all to come to a conclusion of a baseline and must come to a consensus based on individual interpretation.

Likes 0	
Dislikes 0	

Response
Thank you for your support. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	Yes
Document Name	

Comment
The standard drafting team has done an excellent job in addressing stakeholder comments and adjusting the standard language. For R1, R2 and R3 MH suggests beginning each with either “The” or “Each” to match CIP-002, CIP-012 and CIP-013. This is a non-substantive change. The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”: The/Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber

Systems with External Routable Connectivity. The documented process(es) shall provide methods for detecting and evaluating anomalous network activity and shall include each of the following requirement Parts:	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. For Requirements R1, R2, and R3, the DT added the word “Each” at the beginning of the requirements to align with the CIP family of standards.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
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	

Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the SDT's consideration if previous comments submitted. In order to clarify and ensure the measures and requirement language are aligned, Texas RE recommends adding "documented" in front of risk-based rationale in Requirement Part 1.1: 1.1 Implement, using a *documented* risk-based rationale, network data feed(s)…	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Requirement R1 already includes a requirement to "implement one or more documented process(es)" and those "processes shall include each of the following requirement Parts:" Thus the drafting team felt that the risk-based rationale used in Requirement R1, Part 1.1 already requires documentation as part of an entity's INSM process.	

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA recommends adjusting the wording of R2 to eliminate confusing grammar: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to mitigate the risks of unauthorized deletion or modification of internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT modified the language based on previous comments on a prior draft of CIP-015-1. The DT believes that the current grammar is still appropriate.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2.	

It is not clear if the Requirement R2 is expecting both detection of unauthorized access and/or changes along with protection mechanisms to prevent unauthorized access or if the entity can choose what combination of controls is appropriate to them based on their security risk tolerance. BC Hydro recommends to provide clarity in the Requirement R2 to remove ambiguity and scope these accurately. BC Hydro also notes that although Technical Rationale provides examples of guidance it is not an ERO endorsed compliance guidance document. Auditors may chose to adhere to certain aspects from Technical Rationale and choose to leave others.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary. The Technical Rationale has been updated to read: "The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection."	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD recommends the Standards Drafting Team swap Requirements R2 and R3 to better align the requirements in the order they should be implemented. Requirement R2 is to "protect" INSM data against unauthorized deletion in support of Requirement R3. Requirement R3 is to "retain" INSM data associated with network activity determined to be anomalous. The methods to "detect" anomalous network activity should be addressed *before* methods to "protect" INSM data against unauthorized deletion. Therefore, we recommend moving R2 to R3, and R3 to R2. We feel that this change would be non-substantive and could be made in the final ballot.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used: "….to mitigate the risks to the confidentiality, integrity, and availability of the collected data."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	

More clarity is required on which data needs to be protected. What is meant by protection method (mitigation of unauthorized modification)?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale provides additional insights for this. The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary. Compliance with this requirement includes implementation of protective and detective controls.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST recommends that R2 address the protection of collected INSM data both in storage and in transit (e.g., from a substation with medium impact BCS with ERC to a SIEM system located at an entity's headquarters or a Control Center).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment, but did not want to be that prescriptive.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	

R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in the previous draft, Technical Rationale, and FAQ.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in previous draft, Technical Rationale, and FAQ.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in previous draft, Technical Rationale, and FAQ.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used: "….to mitigate the risks to the confidentiality, integrity, and availability of the collected data."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale provides additional insights for this. The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary. Compliance with this requirement includes implementation of protective and detective controls.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No

Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC's comments.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
The wording of requirement R2 and M2 clearly outline the requirements. A non-substantive change is suggested to re-order R2 and R3, so that a future requirement is not referenced. This will make it easier to read the standard in order. If this is adopted, then references to R3 would become R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes

Document Name	
Comment	
NEE agrees with EEI comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes

Document Name	
Comment	
ITC supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Avista agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R2 and Measurement M2.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. Please see responses to EEI's and NAGF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The wording of requirement R2 and M2 clearly outline the requirements. MRO NSRF suggests a non-substantive change to re-order Requirements (and consequently Measures) R2 and R3 so that this requirement refers back to requirements already read vs. both back and forward to a requirement not yet read, making the standard easier to understand when reading it in order. If adopted the reference to R3 would need to be changed to R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
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	

Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments: "We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC's comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	

SRP disagrees with the proposed language in Requirement R3. For example, CIP-007 R4, states that logs are retained for 90 days. The current draft of CIP-015 does not state a time frame to keep logs. How long should REs keep evidence? Should each RE make this determination and possibly write up a policy on saving data for a time frame of their choosing? If that is the case, each RE will be able to keep a different amount of data, some more some less. Would that be acceptable to an auditor or is that the intent of the drafting team? SRP prefers language added in the requirement stating how each RE must store x days of data at minimum or that each RE must retain data to show compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order. Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
R3: SPP asks that the SDT provide additional clarity around what is a reasonable duration for data retention. The current language places the burden on the entity to determine that duration, but records retention for ERO compliance monitoring and enforcement could significantly lengthen how long an entity is required to retain the data and place a significant cost on an entity for storing that data. A more prescriptive time period (e.g., 90 days, 180 days) would seem reasonable to include in the R3 requirement language, and precedence currently exists in the NERC CIP Standards for security event logging today (CIP-007-6, R4, Part 4.3).	
Likes 0	
Dislikes 0	

Response
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy is concerned about the use of the word "detailed" when describing the level of INSM data that should be retained. What information would be required to be retained that is not relevant to the anomalous activity if full packet capture data is not required?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to IRC SRC's comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Ruchi Shah - AES - AES Corporation - 5	

Answer	No
Document Name	
Comment	

AES supports MRO NSRF comments listed below

The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for

double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests **eliminating CIP-015 R3** and **adding a new sub part 1.4** a to read: *1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall* initiate activities identified in its Cyber Security Incident response plan. The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to MRO NSRF's comments.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
See response to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to Question 2.	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	

The SRC is concerned that the language "internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2" is not sufficiently clear and will lead to auditing challenges. The concept of "relevant to anomalous network activity" can be construed in many ways, and different auditors may come to different conclusions regarding the relevance of certain network activity.

To ensure consistency with R1.2 and R1.3, the SRC recommends that the determination of what is "*anomalous"* be left to those sub-requirements and the term *"relevant to"* be replaced with the term "related to". The SRC recommends the following note language revision:

Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not related to network activity detected and evaluated under Requirement R1, Parts 1.2 and 1.3.

It is also unclear what action the phrase "until the action is complete" is intended to refer to, and the SRC recommends that this be clarified.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	

We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	
We would prefer to have a defined timeframe for data retention similar to CIP-007 Requirement R4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	

Comment	
SMECO agrees with ACES comments: Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order.Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA appreciates the clarification in R3 and the Technical Rationale regarding which data must be retained. However, we note that there is potential for voluminous data to be flagged as "anomalous", especially during the time it will take to tune the process. BPA does not support the retention timeframe "until the action is complete." It is unclear if this phrase is referring to the evaluation required by Part 1.3, the determination of further actions required by Part 1.3, or the "further actions" mentioned in Part 1.3. BPA notes that the latter could include risk mitigation or recovery actions that span a considerable length of time.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. If further action is determined to be necessary in accordance with Requirement R1, Part 1.3, the data shall be retained until that further action is completed.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this questions in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	Yes
Document Name	
Comment	
Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. SIGE also appreciates the note at the end of the requirement, as it helps add clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. CEHE also appreciates the note at the end of the requirement, as it helps add clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's and NAGF's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF supports the proposed language for CIP-015-1 Requirement R3 and Measurement M3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI’s comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI's comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
The wording of the Note under Requirement R3 can be improved by revising it to state "(for example, full packet capture data, etc.)", or alternately "(e.g. full packet capture data, etc.)". As the Note is currently written, an entity may assume that "full packet capture" is a	

requirement for internal network security monitoring in Requirement R1, whereas the intent of the Note seems to be to provide an example of the data that is not required to be obtained. This change would be non-substantive and could be made in the final ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE agrees with EEI comment: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation agrees with EEI comments: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Only retaining the data that is associated with network activity determined to be anomalous could lead to a forensics issue if the traffic is within the current baseline and not pre-identified as an anomaly. With the current language of the standard this data would not be retained. Responsible Entities should reevaluate the "normal" traffic baseline on a periodic basis to ensure that they are identifying any anomalous activity to address this risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a "one-size-fits-all" approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro does not believe the note is necessary but does not object to adding the note if it promotes consensus. Manitoba Hydro suggests that the word “detailed” and parenthetical example be removed to clarify and preserve the intent of the note. [Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.]	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Who gets to or how is it determined what data is not relevant? What if an entity doesn't think it was relevant but an auditor does?	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
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	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE understands the phrase “until the action is complete” to mean that if further action is determined to be necessary in accordance with Requirement Part 1.3, the data shall be retained until that further action is completed. Texas RE agrees with retaining network activity determined to be anomalous until the action is completed, except for anomalous activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident. For anomalous network activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident Texas RE recommends setting the retention period to one calendar year after the completion of the action.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged. Anything under CIP-008 process would follow that process and would not be part of the INSM process. Entities should consider CIP-008 when designing their data retention process for proposed Reliability Standard CIP-015-1.

5. Please provide any additional comments for the DT to consider, if desired.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy supports EEI Comments which state: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.	

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	

The Technical Rationale document can use additional editing to align with the edited standards. For example. On Page 6 near the bottom there is a section titled “Data Collection Locations” that in the first sentence redlines out “collection locations” in favor of “feed(s)” which aligns with the standard. Yet the section title continues to focus on “Locations” as well as the content within the section, even though the standard is now related to “feed(s)”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale has been updated to align with the edited proposed Reliability Standard CIP-015-1.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
The Drafting Team should consider requirement language pertaining to the testing of their program put in place to detect anomalous activity on the Responsible Entity’s network to ensure their controls are working properly. The Drafting Team should also consider requirement language pertaining to the ability to detect instances where the protections put in place are not working properly to reduce the response time of the program not functioning as intended similar to CIP-007-6 R4 P4.2.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged. This is an appropriate internal control that the Responsible Entity could implement.	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
Displaying the requirement, parts and subparts in the table format with the "Applicable Systems, Requirements, and Measures," is the preferred formatting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT received positive feedback in not utilizing the table format in proposed Reliability Standard CIP-015-1.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	
Document Name	
Comment	
We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement. FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cybersecurity Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer	
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI’s comments.	
Richard Vendetti - NextEra Energy - 5	

Answer	
Document Name	
Comment	

NEE agrees with EEI comment: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. Please see responses to EEI's comments.

Mike Magruder - Avista - Avista Corporation - 1

Answer	
Document Name	
Comment	

We support EEI's comments:

EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see responses to EEI's comments.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	
Document Name	

Comment

ITC supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see responses to EEI's comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale has been updated to read: ~~The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[2]"~~ The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	

Comment
The NAGF has no additional comments.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	

Comment
NST disagrees with the SDT's decision to demote network baselining from a Requirement to a Measure, which is essentially nothing more than a suggestion, for two reasons: > FERC Order 887 Paragraph 5 states explicitly, "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment." > We are hard-pressed to imagine how anyone using INSM could detect anomalous network behavior without a baseline. To that point, Order 887 Paragraph 12 states, "Establishing baseline network traffic allows entities to define what is and is not normal and expected network activity and determine whether observed anomalous activity warrants further investigation."

Likes 0	
Dislikes 0	

Response
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided

additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including "risk-based rationale" is more encompassing than alternative language proposed by several commenters. Numerous comments were received expressing support for providing flexibility to Responsible Entities to develop their programs without having specific timelines and obligations that may not align to the operations of all Responsible Entities. We provided details in the Technical Rationale that can be used to support the INSM programs for the Responsible Entities. Additionally, the DT updated the Technical Rationale with additional language to clarify the word "baseline" when used to describe anomaly detection technology.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for Question #5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern Company agrees with the additional comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	
Document Name	
Comment	
The standards drafting committee needs develop NERC defined terms and definitions for the following terms: • Anomalous Network activity • Network Data Feeds The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both. The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” The Merriam-Webster dictionary defined anomalous as:	

Anomalous - adjective
1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
Example - Researchers could not explain the anomalous test results.
2 a: of uncertain nature or classification
b: marked by incongruity or contradiction: PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity.

The INSM system may be classified as BCSI or EACMS per the existing processes for each entity.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 is outside of the scope of Project 2023-03.

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	
Document Name	
Comment	

The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE would like to restate that CEHE does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. CEHE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

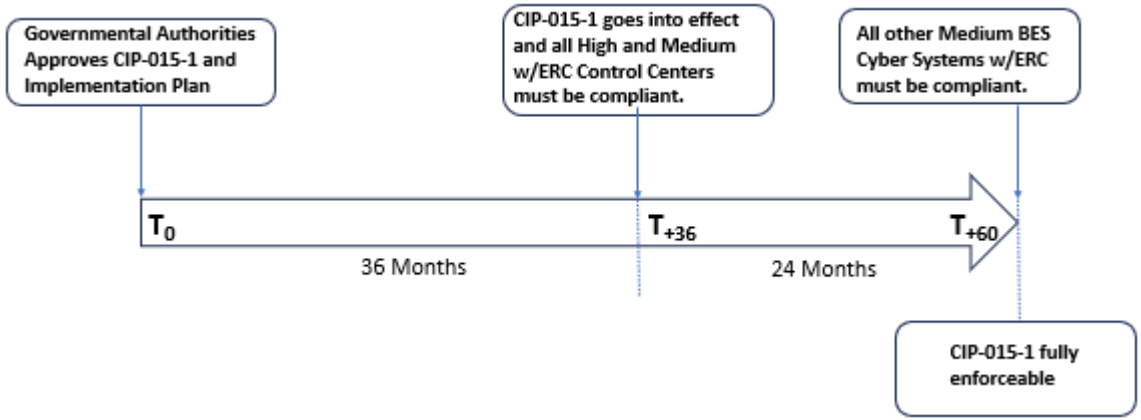
CEHE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please see responses to EEI’s comments.

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations, which may be more challenging to implement.



Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	

SIGE would like to restate that SIGE does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

SIGE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.

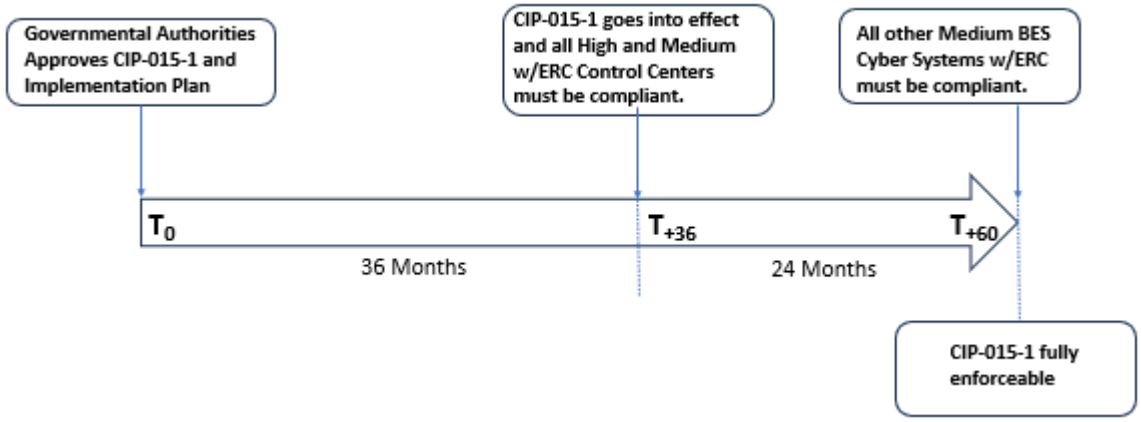
Likes 0	

Dislikes 0	

Response

Thank you for your comments. Please see responses to EEI's comments.

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations, which may be more challenging to implement.



Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	
Implementation Plan: Entities will require sufficient time to research and identify new technology solutions to meet the new INSM requirements. Implementation could require significant changes and/or additions to existing network architectures. Therefore, SPP appreciates and endorses the 36-month timeframe for implementation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
ACES believes the proposed requirements of CIP-015-1 are out of order and should be re-numbered. As currently written, Requirement R2 references Requirements R1 and R3; therefore, ACES believes it should be placed after the current Requirements R1 and R3. ACES would like to thank the SDT for its hard work.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
SRP recommends having baseline defined in the Measures rather than in the technical guidance.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments. The DT provided additional context in the Technical Rationale and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments:	

"The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC's comments.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2023-03 Internal Network Security Monitoring (INSM)

Additional Ballots and Non-binding Poll Open through April 17, 2024

Now Available

Additional ballots for **Project 2023-03 Internal Network Security Monitoring** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Wednesday, April 17, 2024** for the following standard and implementation plan:

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring
  * Requirement R1 was updated to correct an error in the language from "BES Security Systems" to "BES Cyber Systems" to align with the clean version of Draft 2 of CIP-015-1.
- Implementation Plan

The Standards Committee approved waivers to the Standard Processes Manual at their August 2023 meeting, with the additional waiver sought and approved in February 2024. These waivers were sought by NERC Standards for reduced formal comment and ballot periods to assist the drafting team in expediting the standards development process due to firm timeline expectations set by FERC Order No. 887. FERC Order No. 887 was issued under Docket No. RM22-3-000 on January 19, 2023.

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

UPDATED
Standards Announcement
Project 2023-03 Internal Network Security Monitoring (INSM)

Formal Comment Period Open through April 17, 2024

Now Available

A formal comment period for **Project 2023-03 Internal Network Security** is open through **8 p.m. Eastern, Wednesday, April 17, 2024** for the following standard and implementation plan:

- CIP-015-1 – Internal Network Security Monitoring
  * Requirement R1 was updated to correct an error in the language from "BES Security Systems" to "BES Cyber Systems" to align with the clean version of Draft 2 of CIP-015-1.
- Implementation Plan

The standard drafting team's considerations of the responses received from the previous comment period are reflected in this draft of the standard.

Reminder Regarding Corporate RBB Memberships
Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

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 standard and implementation plan, as well as a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 12-17, 2024.**

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2023-03 Internal Network Security Monitoring 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

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/323)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 AB 2 ST
Voting Start Date: 4/12/2024 12:01:00 AM
Voting End Date: 4/17/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 232
Total Ballot Pool: 256
Quorum: 90.63
Quorum Established Date: 4/17/2024 1:47:15 PM
Weighted Segment Value: 76.78

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	74	1	54	0.831	11	0.169	0	4	5
Segment: 2	7	0.6	1	0.1	5	0.5	0	0	1
Segment: 3	59	1	46	0.868	7	0.132	0	4	2
Segment: 4	10	0.9	6	0.6	3	0.3	0	1	0
Segment: 5	57	1	36	0.837	7	0.163	0	4	10
Segment: 6	42	1	27	0.871	4	0.129	0	6	5
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	256	6	175	4.607	37	1.393	0	20	24

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Hydro One Networks, Inc.	Emma Halilovic	Ijad Dewan	Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Negative	Third-Party Comments
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Mia Wilson	Negative	Comments Submitted
3	AEP	Leshel Hutchings		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Calpine Corporation	Whitney Wallace		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Invenergy LLC	Colin Chilcoat		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		None	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 256 of 256 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/323)
Ballot Name: Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan AB 2 OT
Voting Start Date: 4/12/2024 12:01:00 AM
Voting End Date: 4/17/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 230
Total Ballot Pool: 254
Quorum: 90.55
Quorum Established Date: 4/17/2024 1:47:29 PM
Weighted Segment Value: 80.69

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	74	1	52	0.825	11	0.175	0	5	6
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	59	1	45	0.833	9	0.167	0	3	2
Segment: 4	10	0.9	6	0.6	3	0.3	0	1	0
Segment: 5	57	1	35	0.795	9	0.205	0	3	10
Segment: 6	41	1	25	0.806	6	0.194	0	5	5
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.4	4	0.4	0	0	0	2	0
Totals:	254	5.9	172	4.761	39	1.139	0	19	24

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Hydro One Networks, Inc.	Emma Halilovic	Ijad Dewan	Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Negative	Third-Party Comments
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Abstain	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Mia Wilson	Affirmative	N/A
3	AEP	Leshel Hutchings		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Third-Party Comments
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Third-Party Comments
5	Calpine Corporation	Whitney Wallace		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Invenergy LLC	Colin Chilcoat		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		None	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 254 of 254 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/323)
Ballot Name: 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 Non-Binding Poll AB 2 NB
Voting Start Date: 4/12/2024 12:01:00 AM
Voting End Date: 4/17/2024 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 218
Total Ballot Pool: 247
Quorum: 88.26
Quorum Established Date: 4/17/2024 2:51:28 PM
Weighted Segment Value: 79.56

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	72	1	45	0.833	9	0.167	11	7
Segment: 2	7	0.5	1	0.1	4	0.4	1	1
Segment: 3	57	1	37	0.822	8	0.178	8	4
Segment: 4	10	0.9	6	0.6	3	0.3	1	0
Segment: 5	55	1	30	0.789	8	0.211	7	10
Segment: 6	40	1	21	0.808	5	0.192	7	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0
Segment: 10	6	0.4	4	0.4	0	0	2	0
Totals:	247	5.8	144	4.353	37	1.447	37	29

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		None	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Hydro One Networks, Inc.	Emma Halilovic	Ijad Dewan	Abstain	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	Comments Submitted
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Mia Wilson	Negative	Comments Submitted
3	AEP	Leshel Hutchings		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	Comments Submitted
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Santee Cooper	Vicky Budreau		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	Comments Submitted
4	DTE Energy	Patricia Ireland		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	Comments Submitted
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	Comments Submitted
5	Calpine Corporation	Whitney Wallace		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	Comments Submitted
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	National Grid USA	Robin Berry		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Becky Burden		None	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Santee Cooper	Carey Salisbury		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Abstain	N/A
6	Public Utility District No. 1 of Chelan County	Tamarra Hardie		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Santee Cooper	Marty Watson		None	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	Comments Submitted
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 247 of 247 entries

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024
20-day formal comment period with ballot	02/27/2024 – 03/18/2024
10-day formal comment period with ballot	04/05/2024 – 04/17/2024

Anticipated Actions	Date
7-day final ballot	04/24/2024 – 04/30/2024
Board adoption	TBD

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 – Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but is not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1 (1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s) (1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.
R2.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented

				process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.
R3.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

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	03/22/2023
SAR posted for comment	04/06/2023 – 05/05/2023
35-day formal comment period with ballot	12/14/2023 – 01/17/2024
20-day formal comment period with ballot	02/27/2024 – 03/18/2024
10-day formal comment period with ballot	04/05/2024 – 04/17/2024

Anticipated Actions	Date
~~10-day formal comment period with ballot~~	~~04/05/2024 – 04/17/2024~~
~~5~~7-day final ballot	~~TBD~~04/24/2024 – 04/30/2024
Board adoption	TBD

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 – Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

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 Reliability Standard CIP-015-1:

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

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

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 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.

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

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include~~:~~ each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but ~~are~~ is not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

~~M2.~~M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1 (1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s) (1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.
R2.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented

				process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.~~
R3.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification.~~The Responsible Entity did not~~

				~~implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Approved by the NERC Board of Trustees.	

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement ~~R3~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC)[2]. INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address three security issues.

[1] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] *Id.* P 5. (Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment) and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices).

In Order No. 887, FERC directs NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

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 thirty-six (36) 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.

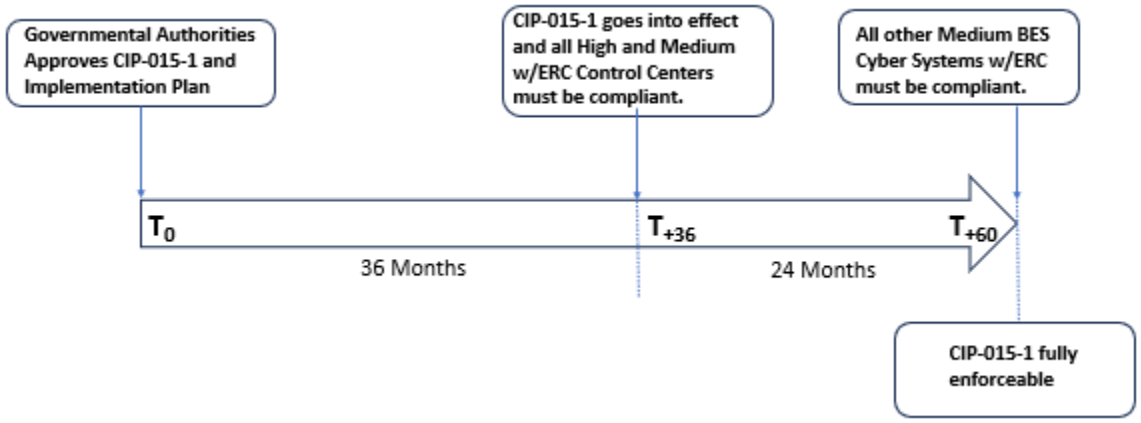
Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1 Parts 1.1. and 1.2. shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It

further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1

Applicable Standard(s)

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Requested Retirement(s)

- None

Applicable Entities

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

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887 directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC)[2]. INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter, to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standard(s) requirement(s) for any new or modified CIP Reliability Standards that address three security issues.

[1] See Applicability Section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

[2] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] *Id.* P 5. (Order No. 887 provides that any new or modified CIP Reliability Standards should: (1) address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment) and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices).

In Order No. 887, FERC directs NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Order No. 887 also directed NERC to conduct a study on the risks of lack of INSM for medium impact BES Cyber Systems without ERC, and all low-impact BES Cyber Systems, and on the challenges and solutions for implementing INSM for those BES Cyber Systems. NERC has completed this study, and it was filed with FERC on January 18, 2024.

General Considerations

This implementation plan reflects consideration that entities will need time to develop and implement Requirements R1, R2, and R3. In order to achieve the objectives of the requirements, all affected Responsible Entities may need to: (1) procure sensors to facilitate the gathering of network data for applicable networks, taking into consideration the availability of products and services by a relatively small vendor marketplace and supply chain challenges; (2) make modifications to networks to better align with the standard; (3) deploy technical solutions to gather network information, which could require outages of operational facilities, which can be challenging to schedule; and (4) implement capabilities to ingest large amounts of network information and perform the necessary analysis. This phased implementation plan is intended to provide additional time to fully comply with Reliability Standard CIP-015-1, prioritizing that the most critical networks, such as Control Centers, are addressed first.

Effective Date and Phased-In Compliance Dates

The effective dates for the proposed Reliability Standard are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below.

Reliability Standard – CIP-015-1 Internal Network Security Monitoring

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 thirty-six (36) 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.

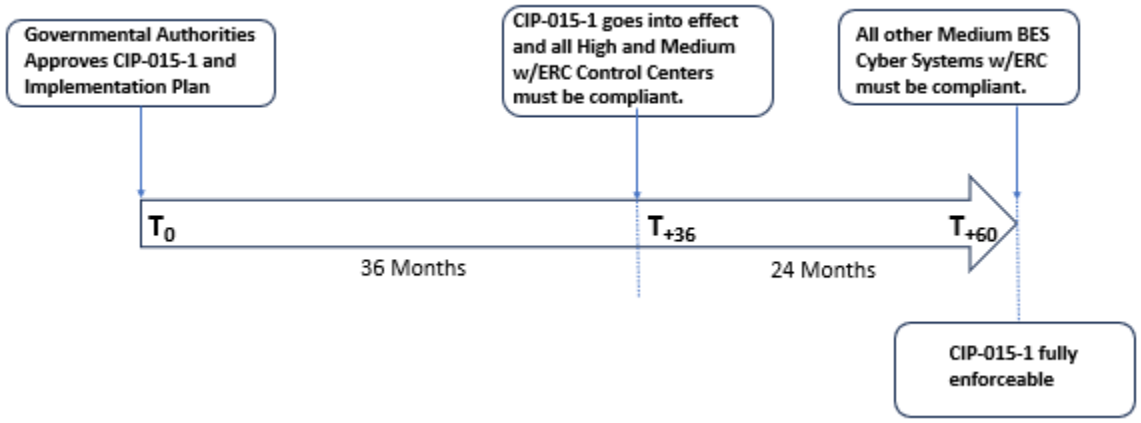
Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for – CIP-015-1 Internal Network Security Monitoring

All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1 Parts 1.1. and ~~R~~1.2. shall initially comply with the requirements in CIP-015-1 for those Control Centers upon the effective date of Reliability Standard CIP-015-1. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It

further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-015-1 within 24 calendar months after the effective date of Reliability Standard CIP-015-1. This phased-in implementation allows for the prioritization of high impact BES Cyber Systems, Control Centers, and backup Control Centers, discussed above, which pose the greatest risk to reliability. It further balances the limited resources, such as available vendors and the added complexity posed by bringing medium impact BES Cyber Systems with External Routable Connectivity into compliance, e.g., increased number of widely separated systems with varying capabilities and connectivity, some power plants may require scheduled outages or upgrades prior to implementing, as well as longer design and testing periods to alleviate risks to generating assets.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es). Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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	The proposed VSL is binary. It does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-015-1, Requirement R2	
Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSL is binary. It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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 Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for ~~the~~ each Responsible Entity to implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es). Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.~~This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.~~
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.~~

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.

VSL Justifications for CIP-015-1, Requirement R2	
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	The proposed VSL is binary. It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	This requirement calls for each Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect INSM data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems. ~~This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.~~
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher risk reliability objective with a lesser risk reliability objective.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. ~~The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain INSM data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, and only reflects the update to the requirement language.
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 VSL is binary. It does 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 VSLs use the same terminology as used in the associated requirement and are, 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	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address three security objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of networks that are internal to the

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following three security objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

operational zones of the Responsible Entity. While the Responsible Entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices that are protected by the ESP of applicable BES Cyber Systems.

Reliability Standard CIP-015-1 requires Responsible Entities to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to anomalous network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation could include escalation to a Responsible Entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. INSM will be an on-going, or possibly an iterative, process enabling Responsible Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887, schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Creation of new Standard CIP-015

At the start of Project 2023-03 – INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In

[3] NERC Glossary of Terms
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with the DT's objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting

reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification
The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM
The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.*

Summary
Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the Responsible Entity for network monitoring purposes.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications."

As described in Richard Bejtlich's book, "The Practice of Network Security Monitoring", monitoring is most effective when collection is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods (Chapters 9-11). In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein Responsible Entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1. specifies that the Responsible Entity identify possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ESP networks and select and implement one or more INSM network data feed(s) in each ESP. These data feeds provide the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.

Network Data Feeds

A network data feed is the combination of a data collection location and a data collection method. Collection methods are technologies that provide visibility of network data to an INSM system (examples are provided below). In context of Reliability Standard CIP-015-1, network locations are physical or virtual devices that move data on a network. These devices include switches, virtual switches, firewalls, routers, network interfaces and similar devices.

Data Collection Locations

Data collection locations may be a physical or a logical concept. In a physical context, network data collection locations connote data collection from devices that move data within and between networks such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. A Responsible Entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the

Responsible Entity may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments.

	High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Considerations for selecting Network Data Feeds

The following considerations might inform the decision for collecting data from a network data feed:

Adversary Analysis

The Responsible Entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive network data feeds that focus on targeted uses cases.

ICS Protocols

The network data feeds, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyze ICS specific protocols.

Data Types

The MITRE ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting network data feeds, a Responsible Entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network data feeds. Consideration of traffic duplication may be part of a rationale on how network data feeds were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data feeds.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network data feeds were selected or excluded for data collection.

A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Parts 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alerts in some INSM systems. Suppressing alarms or data collection may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.
2. High rates of false positive alerts until tuning can be completed.
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the DT these common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

Partner Networks

Transmission Operators have connections to partner networks for the purpose of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some Generator Operators implement connections to external partners for turbine monitoring systems. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value for INSM data collection.

Resilience
While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1. allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN
Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering
Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection
Requirement R1, Part 1.1. does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability
Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a “per system capability” exclusion, Requirement R1, Part 1.1. allows wide latitude to identify INSM network data feeds appropriate to each Responsible Entity’s ESP networks.

Some networks may not have the capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity has several options to provide monitoring data to the INSM including:

- Upgrading hardware and software to systems that do have the capability.
- Installing TAPs to collect network data.

- Collecting flow data.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity.
- Supplementing network data feeds with other pertinent data feeds such as endpoint logs and firewall logs.
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[6].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities are not expected to implement all of these, but rather to choose and implement the network data feeds that provide the most value to the Responsible Entity, as determined by the risk-based rationale in Requirement R1, Part 1.1.

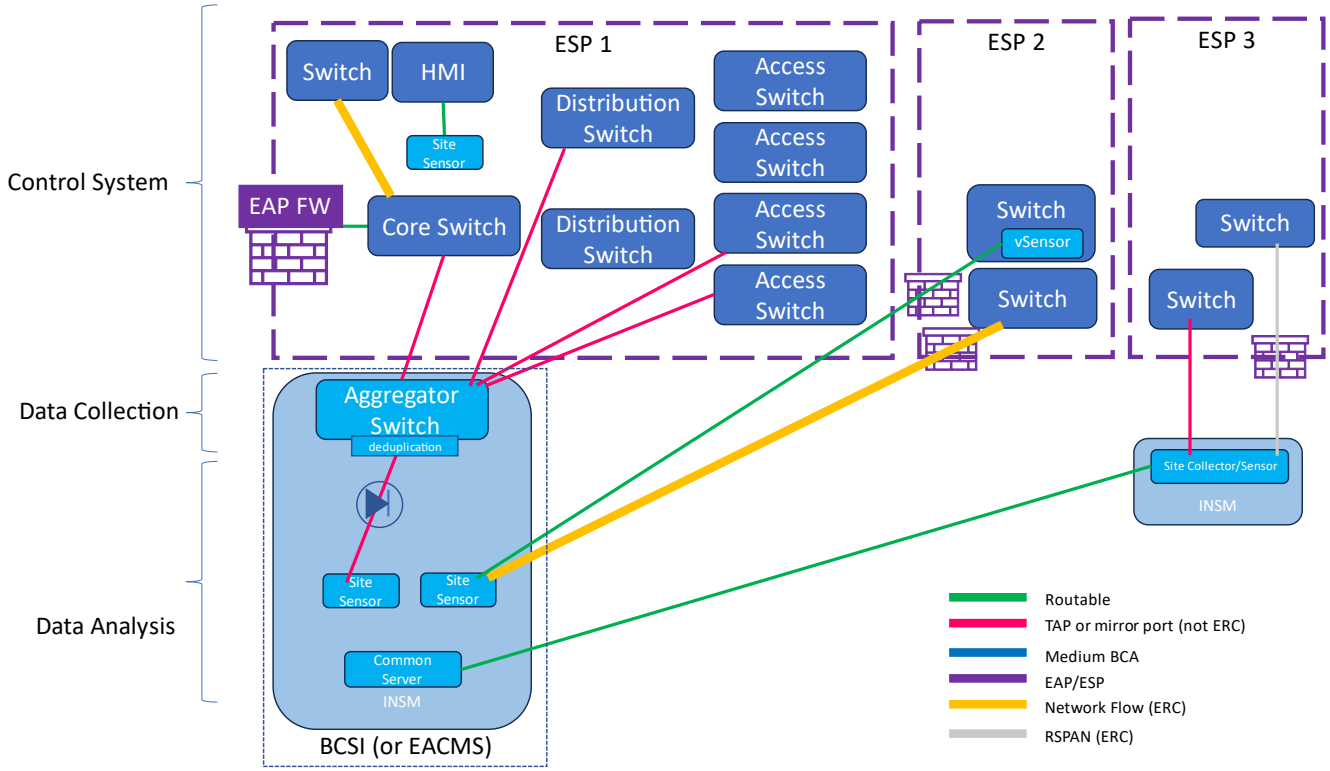


Figure 1

[6] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

This reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new or modified Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of technology advancements, new anomalous detection products are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and INSM Requirement R1 and Requirement R1, Part 1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

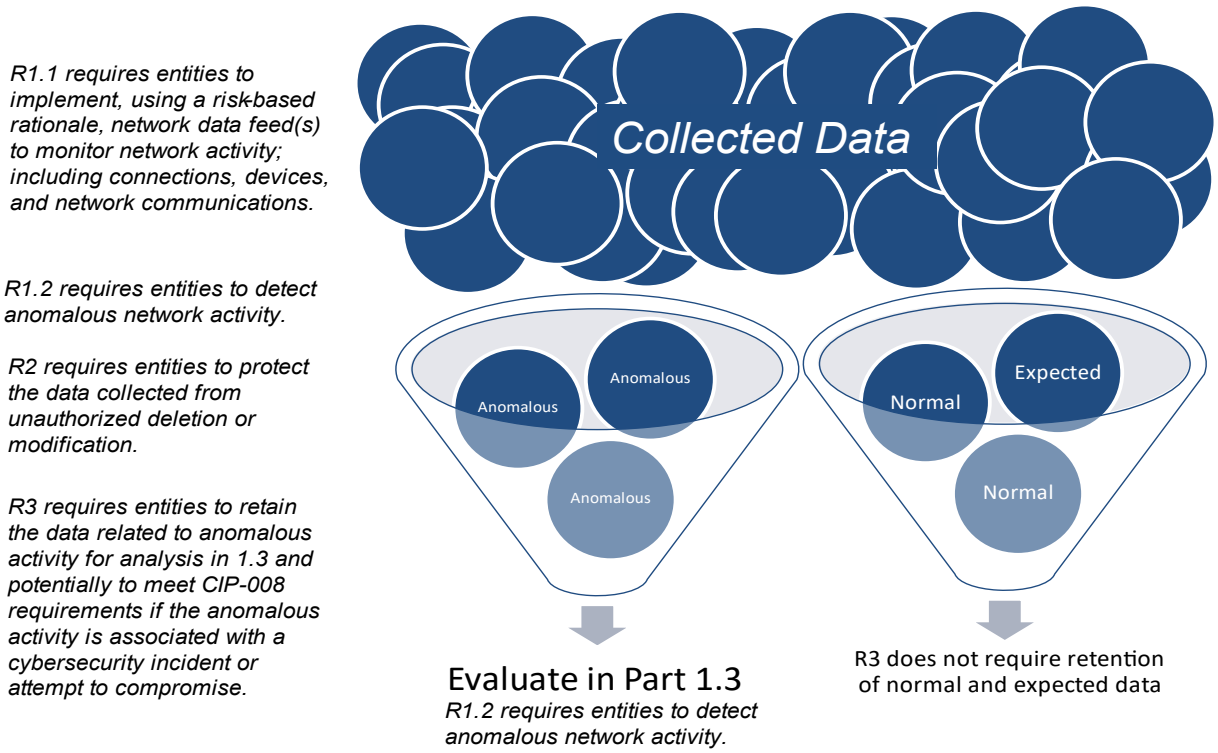


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected

traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Signature-based detections
Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.
When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for data retention in Requirement R3.

Behavioral Detections
Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[7] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning
After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking
INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods
Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods
As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

[7] https://attack.mitre.org/techniques/T0888/

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).
- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning
Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3. "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[8] book. Analyzing the data is an expected part of cyber security operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[8] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

Rationale for Requirement R2

Requirement R2: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3."

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Requirement R2 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide evidence needed to meet CIP-008-6 Requirement R2 for data retention related to an actual Cyber Security Incident or attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system.

Rationale for Requirement R3

Requirement R3: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[9]). The intent of Requirement R3 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system.
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement R3 is intended to limit information sharing. The focus of Requirement R3 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities to share information gathered by INSM systems (see NIST 800-150[10], CISA Information Sharing Guidance[11], Cyber security Information Sharing act of 2015[12]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[13]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities may

[9] https://attack.mitre.org/techniques/T1070/
[10] https://csrc.nist.gov/pubs/sp/800/150/final
[11] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[12] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[13] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf See Page 8

need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feeds to implement as part of Requirement R1, Part 1.1.

The table below uses the following simplified diagram of a high impact ESP network.

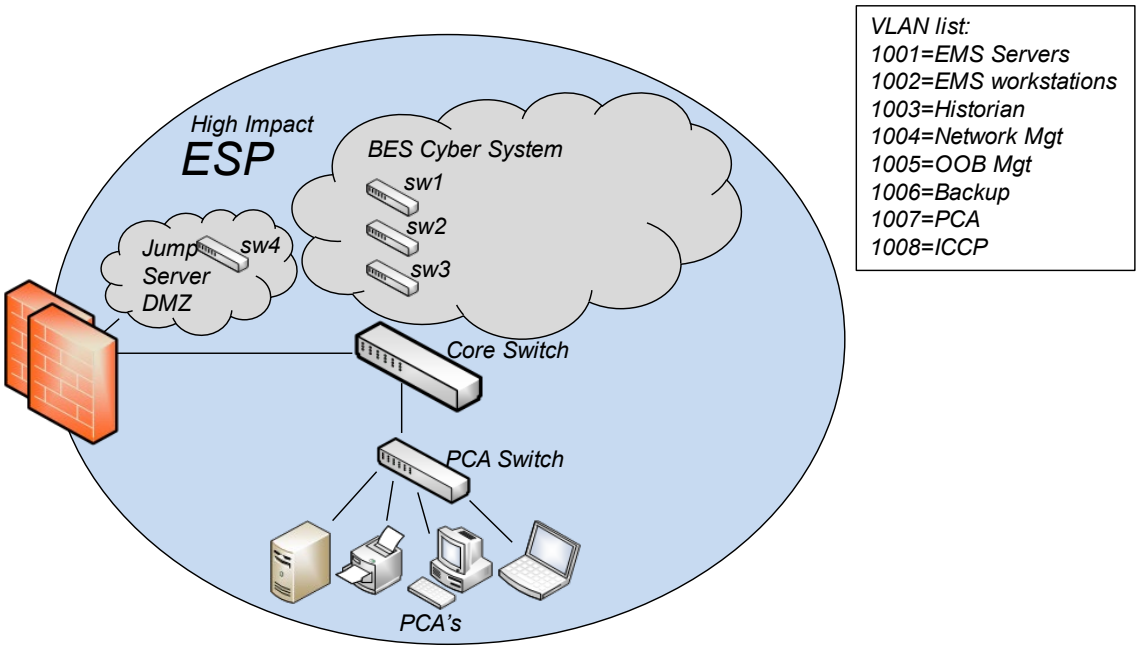


Figure 3

Example rationale for selecting Network Data Feeds:

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports	IRA to the jump server is a likely attack vector.

			to physical port	
	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected

				to be abused by a malicious insider. The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.
Firewall Log data	Yes	Firewall	API	The INSM tool includes a built-in integration to the firewall which provides information about blocked connection attempts.

This example provides some of the considerations for selecting network data feeds. This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.

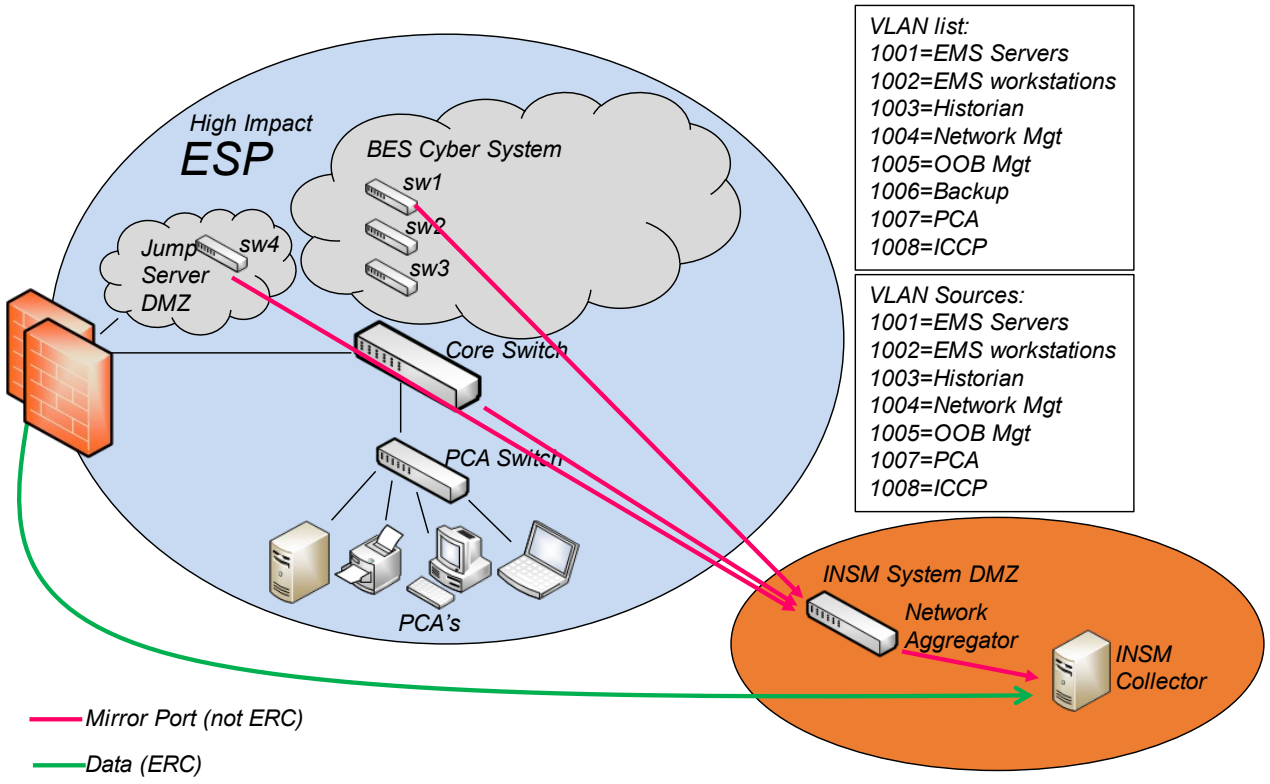

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.
V0.3	24 Apr 2024	Changes based on industry comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address three security objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of networks that are internal to the

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following three ~~3~~ security objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

operational zones of the Responsible Entity. While the Responsible Entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices that are protected by the ESP of applicable BES Cyber Systems.

Reliability Standard CIP-015-1 requires Responsible Entities to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the ~~collection location(s) and method(s)~~ network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to anomalous ~~suspicious~~ network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation could include escalation to a Responsible Entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. INSM will be an on-going, or possibly an iterative, process enabling Responsible Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887, schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Creation of new Standard CIP-015

At the start of Project 2023-03 ~~-~~ INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In

[3] NERC Glossary of Terms
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with the DT's ~~our~~ objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting

reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification

~~The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[6]"~~ The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM

The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.*

Summary

Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the Responsible Entity for network monitoring purposes.

~~[6] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf~~

Rationale for Requirement R1 Part 1.1

*Requirement R1, Part 1.1: "*Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications."

As described in Richard Bejtlich's book, "The Practice of Network Security Monitoring", monitoring is most effective when collection is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods (Chapters 9-11). In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein Responsible Entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1. specifies that the Responsible Entity identify possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ESP networks and select and implement one or more ~~a collection of~~ INSM network data feed(s) in each ESP. These data feeds ~~that~~ provide~~s~~ the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.

Network Data Feeds

A network data feed is the combination of a data collection location and a data collection method. Collection methods are technologies that provide visibility of network data to an INSM system (examples are provided below). In context of Reliability Standard CIP-015-1, network locations are physical or virtual devices that move data on a network. These devices include switches, virtual switches, firewalls, routers, network interfaces and similar devices.

Data Collection Locations

~~In Reliability Standard CIP-015-1, "network data feed(s)"~~Data collection locations may be ~~refers to both~~ a physical ~~and~~ or a logical concept. In a physical context, network data collection locations connote data collection from devices that ~~perform technical functions~~move data within and between networks such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. A Responsible Entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the Responsible Entity may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

~~The Responsible Entity is responsible for identifying physical and logical network data feed(s) that will provide the highest value data for the INSM system.~~

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow.

	Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments. High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Considerations for selecting Network Data Feeds

The following considerations might inform the decision for collecting data from a network data feed:

Adversary Analysis

The Responsible Entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive ~~collection~~ network data feeds that ~~priorities to~~ focus on targeted uses cases ~~that would inform collection locations and exclusions~~.

ICS Protocols

The network data feeds~~collection locations and methods~~, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyze ICS specific protocols.

Data Types

The MITRE ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting ~~data locations and methods~~network data feeds, a Responsible Entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting ~~network collection locations and methods~~network data feeds. Consideration of traffic duplication may be part of a rationale on how ~~network locations~~network data feeds were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data ~~collection locations~~feeds.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network ~~locations~~ data feeds were selected or excluded for data collection.

A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Parts 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alerts in some INSM systems. Suppressing alarms or data collection~~s~~ may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.
2. High rates of false positive alerts until tuning can be completed.
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the DT these

common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

Partner Networks
Transmission Operators have connections to partner networks for the purpose of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some Generator Operators implement connections to external partners for turbine monitoring systems. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value for INSM data collection.

Resilience
While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1. allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN
Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering
Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection
Requirement R1, Part 1.1. does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability
Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a “per system

capability" exclusion, Requirement R1, Part 1.1. allows wide latitude to identify INSM network data feeds ~~collection locations and data collection methods~~ appropriate to each Responsible Entity's ESP networks.

Some networks may not have the capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity has several options to provide monitoring data to the INSM including:

- Upgrading hardware and software to systems that do have the capability.
- Installing TAPs to collect network data.
- Collecting flow data.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity.
- Supplementing network data feeds with other pertinent data feeds such as endpoint logs and firewall logs.
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[7].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities are not expected to implement all of these, but rather to choose and implement the ~~collection locations and methods~~network data feeds that provide the most value to the Responsible Entity, as determined by the risk-based rationale in Requirement R1, Part 1.1.

[7] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

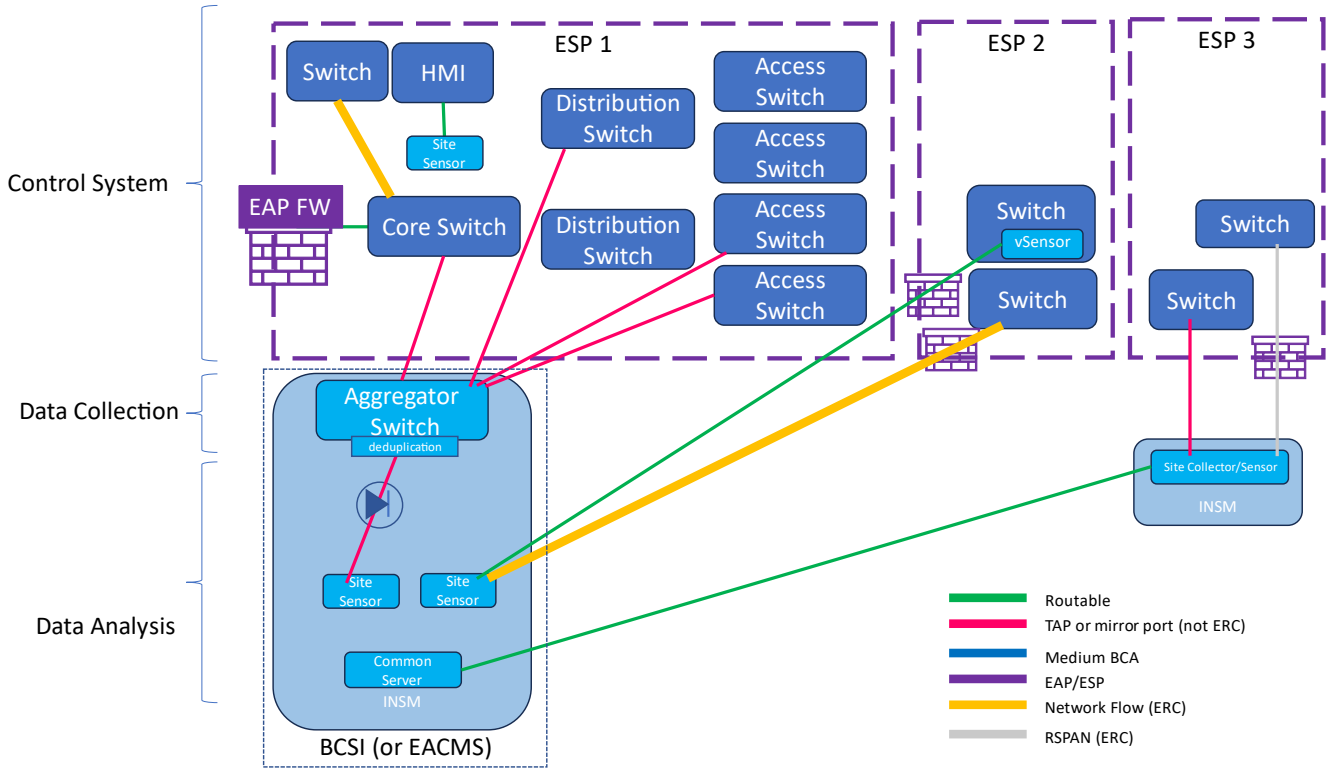


Figure 1

This reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new or modified Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of technology advancements, new anomalous detection products are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

> *Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1."*

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

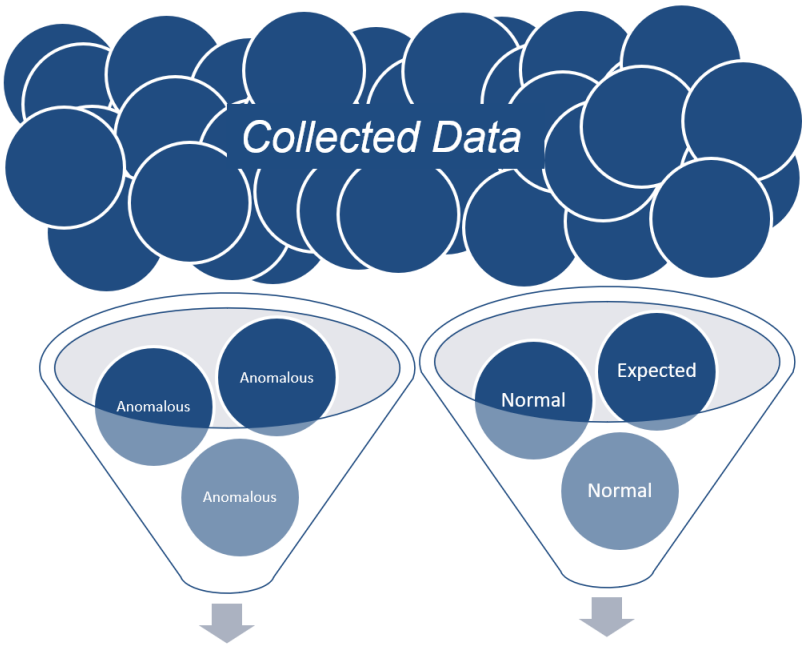
As used in this document and ~~the~~ INSM Requirement R1 and Requirement R1, Part ~~R~~1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

R1.1 requires entities to implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

R1.2 requires entities to detect anomalous network activity.

R2 requires entities to retain the data related to anomalous activity for analysis in 1.3 and potentially to meet CIP-008 requirements if the anomalous activity is associated with a cybersecurity incident or attempt to compromise.

R3 requires entities to protect the data collected from unauthorized deletion or modification.



Evaluate in Part 1.3

R1.2 requires entities to detect anomalous network activity.

R2 does not require retention of normal and expected data

R1.1 requires entities to implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

R1.2 requires entities to detect anomalous network activity.

R2 requires entities to protect the data collected from unauthorized deletion or modification.

R3 requires entities to retain the data related to anomalous activity for analysis in 1.3 and potentially to meet CIP-008 requirements if the anomalous activity is associated with a cybersecurity incident or attempt to compromise.

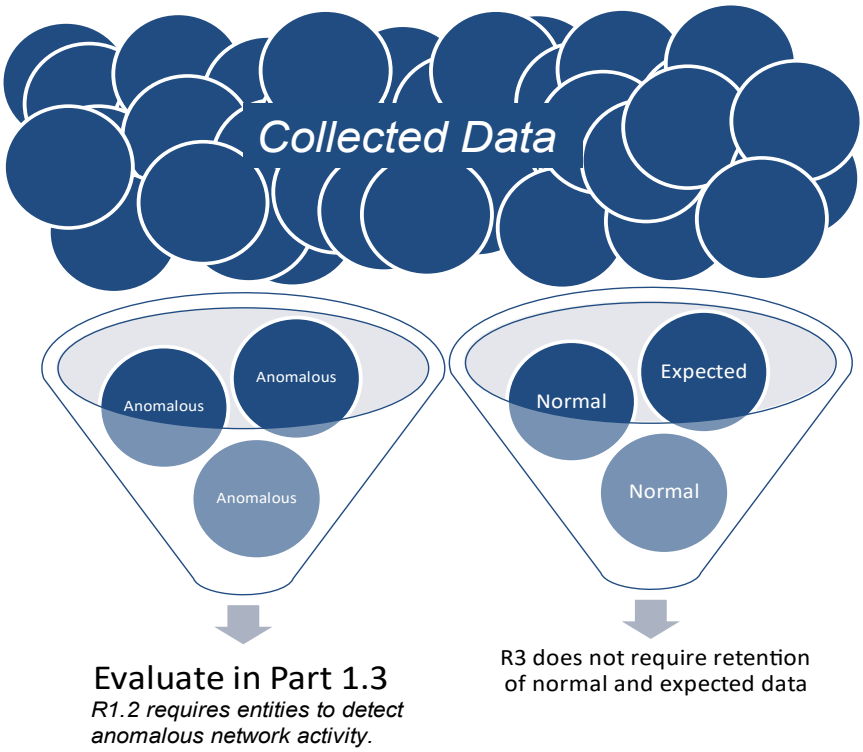


Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Signature-based detections
Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity. When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for data retention in Requirement ~~R2~~R3.

Behavioral Detections
Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[8] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning
After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking
INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods
Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods
As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).
- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

[8] https://attack.mitre.org/techniques/T0888/

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning
Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3. "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[9] book. Analyzing the data is an expected part of cyber security operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[9] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

~~Rationale for Requirement R2~~

> ~~*Requirement R2: "Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification."*~~

~~A common adversary technique is "Indicator Removal" (T1070[10]). The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary.~~

~~Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:~~

- ~~Granting only authorized personnel electronic and physical access to the INSM system.~~
- ~~Installing an INSM system with built-in methods that safeguard the integrity of stored data.~~
- ~~Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.~~
- ~~Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.~~
- ~~Implement two-factor authentication for access to the INSM system.~~
- ~~Other commonly accepted methods used to protect log data.~~

Rationale for Requirement ~~R3~~R2

> *Requirement ~~R3~~R2: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity~~,~~ at a minimum until the action is complete~~,~~ in support of Requirement R1, Part 1.3."*
>
> *Note: The Responsible Entity is not required to retain internal network security monitoring data -that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.*

Requirement ~~R3~~ R2 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. -Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide

~~10 https://attack.mitre.org/techniques/T1070/~~

evidence needed to meet CIP-008-6 Requirement ~~R3~~ R2 for data retention related to an actual Cyber Security Incident or attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system.

Rationale for Requirement R3

Requirement R3: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[11]). The intent of Requirement R3 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system.
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement ~~R2~~ R3 is intended to limit information sharing. The focus of Requirement ~~R2~~ R3 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities to share information gathered by INSM systems (see NIST 800-150[12], CISA Information Sharing Guidance[13], Cyber security Information Sharing act of 2015[14]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[15]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities may

[11] https://attack.mitre.org/techniques/T1070/
[12] https://csrc.nist.gov/pubs/sp/800/150/final
[13] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[14] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[15] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf See Page 8

need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feeds to implement as part of Requirement R1, Part 1.1.

The table below uses the following simplified diagram of a high impact ESP network.

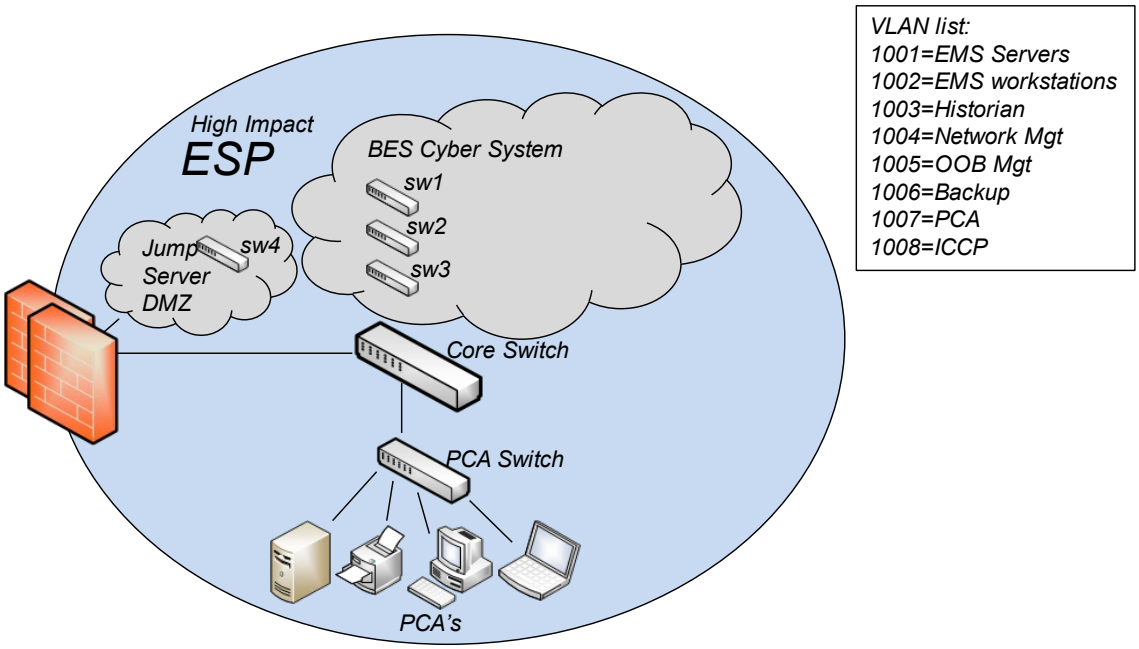


Figure 3

Example rationale for selecting Network Data Feeds:

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports	IRA to the jump server is a likely attack vector.

			to physical port	
	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected

				to be abused by a malicious insider. The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.
Firewall Log data	Yes	Firewall	API	The INSM tool includes a built-in integration to the firewall which provides information about blocked connection attempts.

This example provides some of the considerations for ~~selection~~ selecting network data feeds. This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.

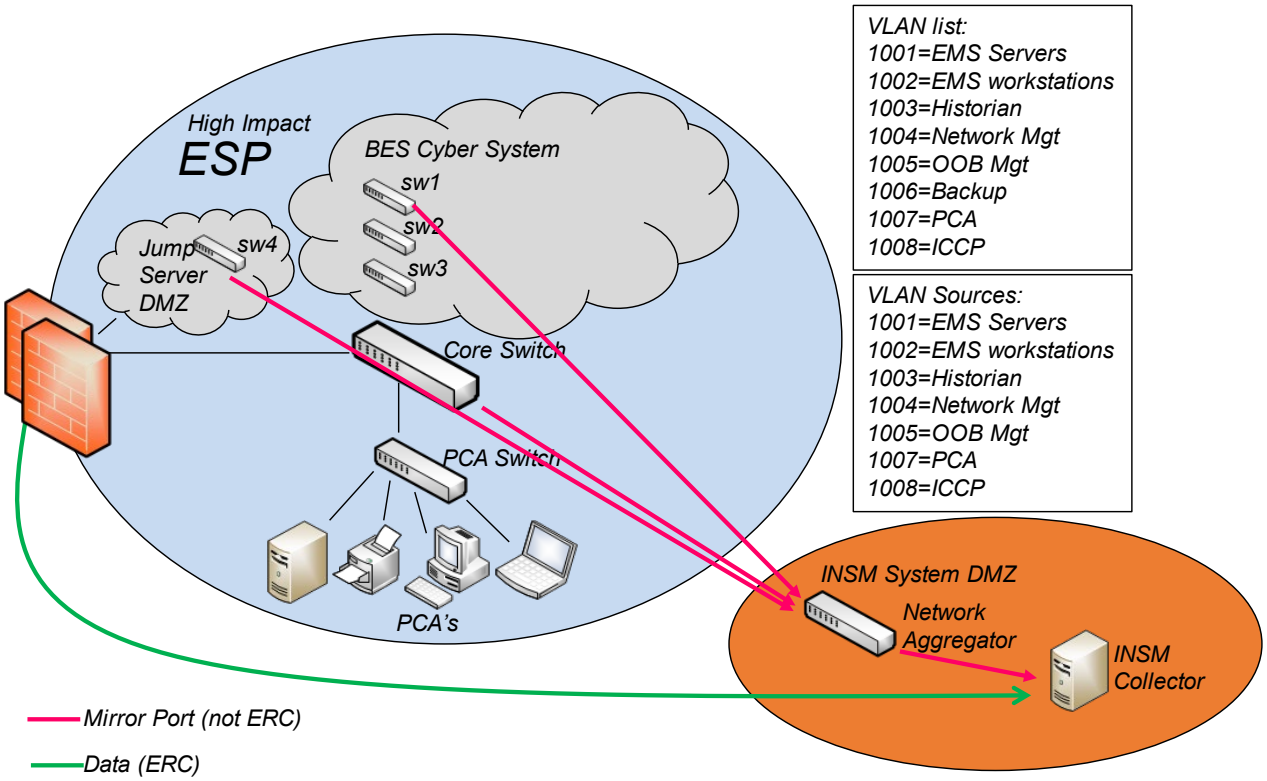

VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.
V0.3	24 Apr 2024	Changes based on industry comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FAQ for Reliability Standard CIP-015-1

April 24, 2024

CIP-015 – Internal Network Security Monitoring

Q – What is internal network security monitoring (INSM)?

INSM refers to a forensic cyber security technology where entities copy network traffic in a trusted network zone, like an Electronic Security Perimeter (ESP), and feed that copied network data to an INSM system that is capable of establishing a pattern of expected network traffic. FERC calls this pattern of expected network traffic a "baseline" in Order No. 887.[1] Once the expected network traffic baseline has been established, subsequent incoming network traffic is compared against the baseline and traffic that does not match the baseline in the INSM system is detected as anomalous and alerted on. These detections require analysis to determine if the anomalous network traffic is normal and benign, abnormal but not suspicious, or potentially malicious. FERC Order No. 887 states that, "INSM consists of three basic phases: (1) collection; (2) detection; and (3) analysis.[2] Taken together, these three stages provide the benefit for early detection and alerting of intrusions and malicious activity."[3]

Q – How is INSM different from traditional intrusion detection systems (IDS)?

Traditional IDS systems are categorized as performing signature-based detection of malicious activities. Similar to traditional anti-virus systems, IDS relies on an understanding of known malicious computer code for detection of malicious activity in a network. Duplicated network traffic fed to an IDS is then compared directly against the known signatures of malicious code implemented in the IDS. If the network traffic matches one of the signatures, an alert is issued. INSM does not typically use signatures of known malicious code. Instead, INSM relies on developing a pattern of expected network traffic and then compares incoming traffic against that pattern to identify potentially malicious traffic.

Additionally, IDS systems do not typically store the network traffic fed to them for further analysis. Network traffic data is usually discarded once the signature comparison takes place. On the other hand, INSM systems are typically capable of storing the network traffic and other metadata associated with the anomalous detection for further analysis and threat hunting while deleting non-anomalous network traffic to reduce storage requirements.

---

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 at P 9.

[3] *Id.* (citing Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2020/applied-collection-framework).

Q – What are the benefits of installing an INSM system?

FERC Order No. 887 paragraphs 10-12 describe the benefits as follow:

> *The benefits of INSM can be understood by first describing the way attackers commonly compromise targets. Attackers typically follow a systematic process of planning and execution to increase the likelihood of a successful compromise. This process includes reconnaissance (e.g., information gathering), choice of attack type and method of delivery (e.g., malware delivered through a phishing campaign), taking control of the entity's systems, and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information). Thus, successful cyberattacks require the attacker to: (1) gain access to a target system; and (2) execute commands while in that system.*
>
> *INSM could better position an entity to detect malicious activity that has circumvented perimeter controls and gained access to the target system. Because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity of the attack and improve the entity's ability to stop the attack at its early phases.*
>
> *By providing visibility of network traffic that may only traverse internally within a trust zone, INSM can warn entities of an attack in progress. For example, properly placed, configured, and tuned INSM capabilities such as intrusion detection system and intrusion prevention system sensors could detect and/or block malicious activity early and alert an entity of the compromise. INSM can also be used to record network traffic for analysis, providing a baseline that an entity can use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal expected network activity and determine whether observed anomalous activity warrants further investigation. The recorded network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious activity.*[4]

[4] *Id.* PP 10-12.

Q – Why did the Drafting Team (DT) choose not to create a NERC Glossary of Terms for "anomalous"?

The DT considered whether or not to create a NERC Glossary of Terms entry for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT determined "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary of Terms.

> "Anomalous - adjective
>
> 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
> Example – Researchers could not explain the anomalous test results.
>
> 2 a: of uncertain nature or classification
>
> b: marked by incongruity or contradiction: PARADOXICAL[2]

Network anomaly detection is a well-known cyber security technique that provides network security threat detection. These systems track critical network characteristics in Real-time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Examples of such characteristics include excessive traffic volume, excessive bandwidth usage, or unusual protocol use. The DT determined that this technology has existed for many years, and it was unnecessary to define the term for industry. Many electric industry entities have already implemented, or are in the process of implementing, network anomaly detection solutions at their facilities. An additional reason for not defining the term is that "anomaly detection" is a phrase used by vendors to describe their proprietary technologies. However, in general, all vendors in the anomaly detection space compare incoming network traffic feeds against a baseline of known expected and normal traffic to detect something that is out of the ordinary, unusual, or unexpected. In a word: anomalous.

Q – Is network traffic required to be captured for Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs)?

The DT focused proposed Reliability Standard CIP-015-1, Requirement R1, on networks protected by an ESP. EACMS and PACS not protected by an entity's defined ESP are outside the scope of Project 2023-03 INSM. One example of EACMS and PACS Cyber Assets that are out of scope of Project 2023-03 INSM would be those existing in a demilitarized zone (DMZ) not protected by the entity's BES Cyber System's ESP(s).

Entities that choose to protect EACMS, PACS, and PCAs with a defined ESP should consider network traffic from those systems to be in scope for proposed Reliability Standard CIP-015-1, Requirement R1. Protected ESP networks connected to EACMS, PACS, and PCAs should be considered for data collection and monitoring for anomalous network traffic, as these systems are not immune from attempts to compromise, and they could serve as pivot points for an attack on a Bulk Electric System (BES) Cyber System protected by the same ESP.

[2] https://www.merriam-webster.com/dictionary/anomalous

Q – What does the DT mean by "network activity"?

In Order No. 887, FERC directed NERC to develop standards to address the need for Responsible Entities to monitor for and detect unauthorized activity, connections, devices, and software. The DT intends for the term "network activity" to represent the connections between devices and software included in the network traffic that an entity is collecting as it passes between hosts that are protected by an ESP.

Q – How should an entity decide which ESP networks to monitor and set up data feeds?

Entities are expected to identify which networks are protected by an ESP and use a risk-based rationale to determine where data feeds should be implemented to provide the best opportunities for detection of malicious activity, as set forth in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1. Entities should document their risk-based rationale for assessing which networks to monitor in their INSM process.

For example, entities may choose not to collect data from networks that only carry backup traffic because workstations and servers do not typically route their normal traffic across that backup network. Otherwise, an entity would likely have to capture and temporarily store tremendous amounts of non-malicious backup traffic. From a risk-based perspective, backup networks pose limited risk and would likely not be a good use case for INSM. Likewise, monitoring of encrypted connections provides limited INSM value because all of the traffic passing on that network connection is encrypted, and INSM would be unable to decrypt and analyze the encrypted packets. An entity will realize more cyber security value, from an INSM perspective, if they monitor the decrypted traffic on the other ports on that switch where the VPN tunnel is connected. Entities need to document these kinds of evaluations of an entity's network as evidence for proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1.

A few examples of high-risk networks that should be given extra consideration for providing data feeds would include network traffic associated with an entity's energy management system (EMS) or distributed control system (DCS) server(s) and workstations, third-party connections, traffic associated with authentication servers (e.g., Active Directory or two-actor authentication systems), and programmable logic controller (PLC)/remote terminal units (RTU) communication paths. Each entity's ESP networks will be unique to that entity; therefore, the DT has left it up to the entity to make risk-based decisions, like those described, to determine what network traffic data feeds should be collected to provide the entity's INSM system with the best opportunity for detecting malicious traffic that could be indicative of an attack in progress.

Q – What is the difference between monitoring in CIP-005-7, CIP-007-6, and CIP-015-1?

Reliability Standard CIP-005-7 is exclusively concerned with the monitoring of ESPs. Reliability Standard CIP-005-7, Requirement R1, Part 1.5 requires entities to monitor at the ESP's Electronic Access Point, "For detecting known or suspected malicious communications for inbound and outbound communications." By specifying "known or suspected malicious traffic," it implies the use of signature-based detection methods for known malicious code. Requirement R1, Part 1.5 does not require monitoring of any traffic that is only passing between Cyber Assets within a defined ESP and is focused on traffic passing through the EAP.

FERC Order No. 887 aims to address this gap in cyber security monitoring by requiring INSM implementation.

Reliability Standard CIP-007-6, Requirement R3, Part 3.1 is focused on implementation of traditional signature-based technologies, such as anti-virus, on Cyber Assets. As noted above, this lack of a requirement for monitoring network traffic in the ESP represents a gap, as entities previously were not required to inspect internal ESP traffic for malicious activity.

While Reliability Standard CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT would contend that most entities are meeting this requirement by logging events at the Cyber Asset level in a security information and event management (SIEM) system. The SIEM may also be used for analysis and retention of those host level events to meet Reliability Standard CIP-007-6, Requirement R4, and allow for detection of login attempts and malicious code on those Cyber Assets themselves. INSM would likely be unable to determine whether a login attempt failed or definitively detect malicious code installed on a Cyber Asset and is not a suitable technology to meet Reliability Standard CIP-007-6, Requirement R4, Part 4.1.

Proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1. will require entities to implement the method(s) of their choice to feed the network traffic the entity identified for capture in a defined ESP to a system that can identify patterns of expected network behavior. For proposed Requirement R1 Part 1.2, the INSM detects network traffic from the data feeds that is anomalous based on a comparison with the INSM system's patterns of expected network behavior. Network data associated with an anomalous detection should be protected and retained at least until the required evaluation can be completed in proposed Requirement R1, Part 1.3. The detection should be evaluated and triaged appropriately in proposed Requirement R1, Part 1.3. The DT considers proposed Reliability Standard CIP-015-1 to be an additional cyber security control that can increase the probability of detecting malicious activity in networks protected by an ESP.

Q – What data are entities required to retain and for how long?

Proposed Requirement R2 requires an INSM system to be able to store network traffic data and other metadata associated with each detection of anomalous activity. Data associated with non-anomalous traffic is not required to be retained. Most modern INSM systems are capable of saving just the data associated with anomalous network activity and discarding the rest.

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed by the entity not to be malicious do not need to be further retained after they have been evaluated in proposed Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's Reliability Standard CIP-008 incident response process(es) for further investigation. **Note:** Reliability Standard CIP-008 has its own retention requirements that entities need to keep in mind as they develop their proposed Reliability Standard CIP-015-1 retention process(es).

Q – How does the DT intend for entities to protect INSM data?

FERC Order No. 887 directed NERC to implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. In DT discussions it was clear that the intent was to protect the anomalous network data collected from being tampered with or removed by an adversary such that an entity could not accurately complete the required evaluation in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Malicious actors typically attempt to hide their tracks by removing evidence on a host system. Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.

Entities must protect their INSM data from unauthorized deletion or modification in support of proposed Requirements R1 and R2. Typically, this is done through the use of cyber and physical security controls. Entities should restrict electronic access to the INSM system and INSM data to only those with a need to access it. Restricting physical access to the INSM system is another good control. Use network segmentation to ensure that the INSM system is not part of the same networks the INSM system is monitoring. File integrity monitoring is another option to consider. Entities have developed a range of controls, and the controls they implement should be in line with their existing information protection programs.

Entities will need to assess the data being collected, and the meta data created by an INSM system, to determine if it needs to be protected as BES Cyber System Information (BCSI). Entities that declare the information stored in their INSM system as BCSI and protect the INSM data with their BCSI information protection procedures developed for Reliability Standard CIP-011-2, should meet proposed Reliability Standard CIP-015-1, Requirement R3. If an entity decides that the information is not BCSI, they must apply and document the security protections employed to protect the INSM data from modification or deletion.

Q – Why did the DT not include language that would allow a Technical Feasibility Exception (TFE) in situations where an entity believes they cannot implement INSM?

The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity's ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years.

Q – Is CIP-015-1 cost-effective?

In consideration of the cost effectiveness of proposed Reliability Standard CIP-015-1, the DT provided flexibility to entities to design their INSM systems to meet the proposed Reliability Standard CIP-015-1 requirements no matter the configuration of the individual networks protected by ESPs. Modern control center/data center environments should be capable of replicating an ESP's network traffic. Virtualized

systems should have the capability to replicate internal traffic between Virtual Cyber Assets to an INSM system. Replacing a switch or substation network device to replicate network traffic at key network convergence points is typically an inconsequential expense for an entity. The DT concluded that the main expense will most likely be procurement of INSM software and/or hardware, installation, labor cost, and tuning the system prior to the proposed Reliability Standard CIP-015-1 enforcement date.

The DT provided an implementation timeframe of 36 months for high impact and medium impact with External Routable Connectivity (ERC) control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those substation locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cyber security Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Q – Do entities have to capture traffic for serial connections?

As stated in the Technical Rationale, proposed Requirement R1 does not require collection of data such as serial communications, 4-20 ma circuits, or wide area network circuits such as multiprotocol label switching (MPLS) and other similar technologies.

[3] *Incentives for Advanced Cyber security Investment,* Order No. 893, 183 FERC ¶ 61,033, *order on reh'g,* Order No 893-A*,* 184 FERC ¶ 61.053 (2023); *see* e.g., FERC Cyber security Incentives web page - https://www.ferc.gov/cybersecurity-incentives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FAQ for Reliability Standard CIP-015-1

April ~~5~~24, 2024

CIP-015 – Internal Network Security Monitoring

Q – What is internal network security monitoring (INSM)?

INSM refers to a forensic cyber security technology where entities copy network traffic in a trusted network zone, like an Electronic Security Perimeter (ESP), and ~~redirect~~ feed that copied network data to an INSM system that is capable of establishing a pattern of expected network traffic. FERC calls this pattern of expected network traffic a "baseline" in Order No. 887.[1] Once the expected network traffic baseline has been established, subsequent incoming network traffic is compared against the baseline and traffic that does not match the baseline in the INSM system is detected as anomalous and alerted on. These detections require analysis to determine if the anomalous network traffic is normal and benign, abnormal but not suspicious, or potentially malicious. FERC Order No. 887 states that, "INSM consists of three basic phases: (1) collection; (2) detection; and (3) analysis.[2] Taken together, these three stages provide the benefit for early detection and alerting of intrusions and malicious activity."[3]

Q – How is INSM different from traditional intrusion detection systems (IDS)?

Traditional IDS systems are categorized as performing signature-based detection of malicious activities. Similar to traditional anti-virus systems, IDS relies on an understanding of known malicious computer code for detection of malicious activity in a network. Duplicated network traffic ~~sent~~ fed to an IDS is then compared directly against the known signatures of malicious code implemented in the IDS. If the network traffic matches one of the signatures, an alert is issued. INSM does not typically use signatures of known malicious code. Instead, INSM relies on developing a pattern of expected network traffic and then compares incoming traffic against that pattern to identify potentially malicious traffic.

Additionally, IDS systems do not typically store the network traffic fed to them for further analysis. Network traffic data is usually discarded once the signature comparison takes place. On the other hand, INSM systems are typically capable of storing the network traffic and other metadata associated with the anomalous detection for further analysis and threat hunting while deleting non-anomalous network traffic to reduce storage requirements.

---

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Order No. 887 at P 9.

[3] *Id.* (citing Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2020/applied-collection-framework).

Q – What are the benefits of installing an INSM system?

FERC Order No. 887 paragraphs 10-12 describe the benefits as follow:

> *"The benefits of INSM can be understood by first describing the way attackers commonly compromise targets. Attackers typically follow a systematic process of planning and execution to increase the likelihood of a successful compromise. This process includes reconnaissance (e.g., information gathering), choice of attack type and method of delivery (e.g., malware delivered through a phishing campaign), taking control of the entity's systems, and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information). Thus, successful cyberattacks require the attacker to: (1) gain access to a target system; and (2) execute commands while in that system.*
>
> *INSM could better position an entity to detect malicious activity that has circumvented perimeter controls and gained access to the target system. Because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity of the attack and improve the entity's ability to stop the attack at its early phases.*
>
> *By providing visibility of network traffic that may only traverse internally within a trust zone, INSM can warn entities of an attack in progress. For example, properly placed, configured, and tuned INSM capabilities such as intrusion detection system and intrusion prevention system sensors could detect and/or block malicious activity early and alert an entity of the compromise. INSM can also be used to record network traffic for analysis, providing a baseline that an entity can use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal expected network activity and determine whether observed anomalous activity warrants further investigation. The recorded network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious activity."*[4]

[4] *Id.* PP 10-12.

Q – Why did the Drafting Team (DT) choose not to create a NERC Glossary of Terms for "anomalous"?

The DT considered whether or not to create a NERC Glossary of Terms entry for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT determined "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary of Terms.

> "Anomalous - adjective
>
> 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
> Example – Researchers could not explain the anomalous test results.
>
> 2 a: of uncertain nature or classification
>
> b: marked by incongruity or contradiction: PARADOXICAL[2]

Network anomaly detection is a well-known cyber security technique that provides network security threat detection. These systems track critical network characteristics in Real-time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Examples of such characteristics include excessive traffic volume, excessive bandwidth usage, or unusual protocol use. The DT determined that this technology has existed for many years, and it was unnecessary to define the term for industry. Many electric industry entities have already implemented, or are in the process of implementing, network anomaly detection solutions at their facilities. An additional reason for not defining the term is that "anomaly detection" is a phrase used by vendors to describe their proprietary technologies. However, in general, all vendors in the anomaly detection space compare incoming network traffic feeds against a baseline of known expected and normal traffic to detect something that is out of the ordinary, unusual, or unexpected. In a word: anomalous.

Q – Is network traffic required to be captured for Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs)?

The DT focused proposed Reliability Standard CIP-015-1, Requirement R1, on networks protected by an ESP. EACMS and PACS not protected by an entity's defined ESP are outside the scope of Project 2023-03 INSM. One example of EACMS and PACS Cyber Assets that are out of scope of Project 2023-03 INSM would be those existing in a demilitarized zone (DMZ) not protected by the entity's BES Cyber System's ESP(s).

Entities that choose to protect EACMS, PACS, and PCAs with a defined ESP should consider network traffic from those systems to be in scope for proposed Reliability Standard CIP-015-1, Requirement R1. Protected ESP networks connected to EACMS, PACS, and PCAs should be considered for data collection and monitoring for anomalous network traffic, as these systems are not immune from attempts to compromise, and they could serve as pivot points for an attack on a Bulk Electric System (BES) Cyber System protected by the same ESP.

[2] https://www.merriam-webster.com/dictionary/anomalous

Q – What does the DT mean by "network activity"?

In Order No. 887, FERC directed NERC to develop standards to address the need for Responsible Entities to monitor for and detect unauthorized activity, connections, devices, and software. The DT intends for the term "network activity" to represent the connections between devices and software included in the network traffic that an entity is collecting as it passes between hosts that are protected by an ESP.

Q – How should an entity decide which ESP networks to monitor and set up data feeds?

Entities are expected to identify which networks are protected by an ESP and use a risk-based rationale to determine where data feeds should be implemented to provide the best opportunities for detection of malicious activity, as set forth in ~~-~~proposed Reliability Standard CIP-015-1, Requirement R1, Part ~~R~~1.1. Entities should document their risk-based rationale for assessing which networks to monitor in their INSM process.

For example, entities may choose not to collect data from networks that only carry backup traffic because workstations and servers do not typically route their normal traffic across that backup network. Otherwise, an entity would likely have to capture and temporarily store tremendous amounts of non-malicious backup traffic. From a risk-based perspective, backup networks pose limited risk and would likely not be a good use case for INSM. Likewise, monitoring of encrypted connections provides limited INSM value because all of the traffic passing on that network connection is encrypted, and INSM would be unable to decrypt and analyze the encrypted packets. An entity will realize more cyber security value, from an INSM perspective, if they monitor the decrypted traffic on the other ports on that switch where the VPN tunnel is connected. Entities need to document these kinds of evaluations of an entity's network as evidence for proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1.

A few examples of high-risk networks that should be given extra consideration for providing data feeds would include network traffic associated with an entity's energy management system (EMS) or distributed control system (DCS) server(s) and workstations, third-party connections, traffic associated with authentication servers (e.g., Active Directory or two-actor authentication systems~~)~~, and programmable logic controller (PLC)/remote terminal units (RTU) communication paths~~)~~. Each entity's ESP networks will be unique to that entity; therefore, the DT has left it up to the entity to make risk-based decisions, like those described, to determine what network traffic data feeds should be collected to provide the entity's INSM system with the best opportunity for detecting malicious traffic that could be indicative of an attack in progress.

Q – What is the difference between monitoring in CIP-005-7, CIP-007-6, and CIP-015-1?

Reliability Standard CIP-005-7 is exclusively concerned with the monitoring of ESPs. Reliability Standard CIP-005-7, Requirement R1, Part 1.5 requires entities to monitor at the ESP's Electronic Access Point, "For detecting known or suspected malicious communications for inbound and outbound communications." By specifying "known or suspected malicious traffic," it implies the use of signature-based detection methods for known malicious code. Requirement R1, Part 1.5 does not require monitoring of any traffic that is only passing between Cyber Assets within a defined ESP and is focused on traffic passing through the EAP.

FERC Order No. 887 aims to address this gap in cyber security monitoring by requiring INSM implementation.

Reliability Standard CIP-007-6, Requirement R3, Part 3.1 is focused on implementation of traditional signature-based technologies, such as anti-virus, on Cyber Assets. As noted above, this lack of a requirement for monitoring network traffic in the ESP represents a gap, as entities previously were not required to inspect internal ESP traffic for malicious activity.

While Reliability Standard CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT would contend that most entities are meeting this requirement by logging events at the Cyber Asset level in a security information and event management (SIEM) system. The SIEM may also be used for analysis and retention of those host level events to meet Reliability Standard CIP-007-6, Requirement R4, and allow for detection of login attempts and malicious code on those Cyber Assets themselves. INSM would likely be unable to determine whether a login attempt failed or definitively detect malicious code installed on a Cyber Asset and is not a suitable technology to meet Reliability Standard CIP-007-6, Requirement R4, Part 4.1.

Proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1. will require entities to implement the method(s) of their choice to ~~copy~~ feed the network traffic the entity identified for capture in a defined ESP to a system that can identify patterns of expected network behavior. For proposed Requirement R1 Part 1.2, the INSM detects network traffic from the data feeds that is anomalous based on a comparison with the INSM system's patterns of expected network behavior. Network data associated with an anomalous detection should be protected and retained at least until the required evaluation can be completed in proposed Requirement R1, Part 1.3. The detection should be evaluated and triaged appropriately in proposed Requirement R1, Part 1.3. The DT considers proposed Reliability Standard CIP-015-1 to be an additional cyber security control that can increase the probability of detecting malicious activity in networks protected by an ESP.

Q – What data are entities required to retain and for how long?

Proposed Requirement ~~R3~~ R2 requires an INSM system to be able to store network traffic data and other metadata associated with each detection of anomalous activity. Data associated with non-anomalous traffic is not required to be retained. Most modern INSM systems are capable of saving just the data associated with anomalous network activity and discarding the rest.

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed by the entity not to be malicious do not need to be further retained after they have been evaluated in proposed Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's Reliability Standard CIP-008 incident response process(es) for further investigation. **Note:** Reliability Standard CIP-008 has its own retention requirements that entities need to keep in mind as they develop their proposed Reliability Standard CIP-015-1 retention process(es).

Q – How does the DT intend for entities to protect INSM data?

FERC Order No. 887 directed NERC to implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. In DT discussions it was clear that the intent was to protect the anomalous network data collected from being tampered with or removed by an adversary such that an entity could not accurately complete the required evaluation in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Malicious actors typically attempt to hide their tracks by removing evidence on a host system. Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.

Entities must protect their INSM data from unauthorized deletion or modification in support of proposed Requirements R1 and ~~R3~~R2. Typically, this is done through the use of cyber and physical security controls. Entities should restrict electronic access to the INSM system and INSM data to only those with a need to access it. Restricting physical access to the INSM system is another good control. Use network segmentation to ensure that the INSM system is not part of the same networks the INSM system is monitoring. File integrity monitoring is another option to consider. Entities have developed a range of controls, and the controls they implement should be in line with their existing information protection programs.

Entities will need to assess the data being collected, and the meta data created by an INSM system, to determine if it needs to be protected as BES Cyber System Information (BCSI). Entities that declare the information stored in their INSM system as BCSI and protect the INSM data with their BCSI information protection procedures developed for Reliability Standard CIP-011-2, should meet proposed Reliability Standard CIP-015-1, Requirement ~~R2~~R3. If an entity decides that the information is not BCSI, they must apply and document the security protections employed to protect the INSM data from modification or deletion.

Q – Why did the DT not include language that would allow a Technical Feasibility Exception (TFE) in situations where an entity believes they cannot implement INSM?

The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity's ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years.

Q – Is CIP-015-1 cost-effective?

In consideration of the cost effectiveness of proposed Reliability Standard CIP-015-1, the DT provided flexibility to entities to design their INSM systems to meet the proposed Reliability Standard CIP-015-1 requirements no matter the configuration of the individual networks protected by ESPs. Modern control center/data center environments should be capable of replicating an ESP's network traffic. Virtualized

systems should have the capability to replicate internal traffic between Virtual Cyber Assets to an INSM system. Replacing a switch or substation network device to replicate network traffic at key network convergence points is typically an inconsequential expense for an entity. The DT concluded that the main expense will most likely be procurement of INSM software and/or hardware, installation, labor ~~count and~~ cost, and tuning the system prior to the proposed Reliability Standard CIP-015-1 enforcement date.

The DT provided an implementation timeframe of 36 months for high impact and medium impact with External Routable Connectivity (ERC) control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those substation locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cyber security Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Q – Do entities have to capture traffic for serial connections?

As stated in the Technical Rationale, proposed Requirement R1 does not require collection of data such as serial communications, 4-20 ma circuits, or wide area network circuits such as multiprotocol label switching (MPLS) and other similar technologies.

[3] *Incentives for Advanced Cyber security Investment,* Order No. 893, 183 FERC ¶ 61,033, *order on reh'g,* Order No 893-A, 184 FERC ¶ 61.053 (2023); *see* e.g., FERC Cyber security Incentives web page - https://www.ferc.gov/cybersecurity-incentives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2023-03 Internal Network Security Monitoring (INSM)

Final Ballots Open through April 30, 2024

Now Available

A seven-day final ballot for **Project 2023-03 Internal Network Security Monitoring** is open through **8 p.m. Eastern, Tuesday, April 30, 2024** for the following standard and implementation plan:

- CIP-015-1 – Cyber Security – Internal Network Security Monitoring
  *Please Note: The DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.
- Implementation Plan

The Standards Committee approved waivers to the Standard Processes Manual at their August 2023 meeting, with the additional waiver approved in February 2024. These waivers were sought by NERC Standards for reduced formal comment and ballot periods to assist the drafting team in expediting the standards development process due to firm timeline expectations set by FERC Order No. 887. FERC Order No. 887 was issued under Docket No. RM22-3-000 on January 19, 2023.

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 standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

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

For more information or assistance, contact Senior Standards Developer, Laura Anderson (via email) or at 404-782-1870.

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: 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 FN 3 ST
Voting Start Date: 4/24/2024 8:22:46 AM
Voting End Date: 4/30/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 239
Total Ballot Pool: 256
Quorum: 93.36
Quorum Established Date: 4/24/2024 8:42:10 AM
Weighted Segment Value: 76.57

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	74	1	59	0.855	10	0.145	0	3	2
Segment: 2	7	0.6	0	0	6	0.6	0	0	1
Segment: 3	59	1	49	0.891	6	0.109	0	3	1
Segment: 4	10	0.9	6	0.6	3	0.3	0	1	0
Segment: 5	57	1	40	0.87	6	0.13	0	3	8
Segment: 6	42	1	29	0.879	4	0.121	0	5	4
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	256	6	188	4.594	35	1.406	0	16	17

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Hydro One Networks, Inc.	Emma Halilovic	Ijad Dewan	Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Negative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Negative	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Negative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Mia Wilson	Negative	N/A
3	AEP	Leshel Hutchings		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	N/A
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	N/A
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	N/A
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	N/A
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	N/A
5	Calpine Corporation	Whitney Wallace		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	N/A
5	Santee Cooper	Carey Salisbury		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Invenergy LLC	Colin Chilcoat		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 256 of 256 entries

BALLOT RESULTS

Ballot Name: Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan FN 3 OT
Voting Start Date: 4/24/2024 8:23:09 AM
Voting End Date: 4/30/2024 8:00:00 PM
Ballot Type: OT
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 237
Total Ballot Pool: 254
Quorum: 93.31
Quorum Established Date: 4/24/2024 8:42:13 AM
Weighted Segment Value: 82.1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	74	1	57	0.851	10	0.149	0	4	3
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	59	1	47	0.855	8	0.145	0	3	1
Segment: 4	10	0.9	6	0.6	3	0.3	0	1	0
Segment: 5	57	1	38	0.826	8	0.174	0	3	8
Segment: 6	41	1	26	0.813	6	0.188	0	5	4
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	0	0	0	0	0	0	0	0	0
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	6	0.4	4	0.4	0	0	0	2	0
Totals:	254	5.9	183	4.844	36	1.056	0	18	17

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Allete - Minnesota Power, Inc.	Hillary Creurer		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arkansas Electric Cooperative Corporation	Emily Corley		Abstain	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	N/A
1	Central Iowa Power Cooperative	Kevin Lyons		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	Edison International - Southern California Edison Company	Robert Blackney		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Hydro One Networks, Inc.	Emma Halilovic	Ijad Dewan	Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Negative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Marcus Sabo	Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Long Island Power Authority	Isidoro Behar		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	Rebika Yitna	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Abstain	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Platte River Power Authority	Marissa Archie		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	N/A
1	Santee Cooper	Chris Wagner		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Southern Maryland Electric Cooperative	Roger Perkins		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	ISO New England, Inc.	John Pearson	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Mia Wilson	Affirmative	N/A
3	AEP	Leshel Hutchings		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Ayslynn Mcavoy		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Basin Electric Power Cooperative	Derik Youngs		None	N/A
3	BC Hydro and Power Authority	Ming Jiang		Negative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	N/A
3	Buckeye Power, Inc.	Tom Schmidt	Ryan Strom	Negative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Negative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Entergy	James Keele		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Negative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Affirmative	N/A
3	Manitoba Hydro	Mike Smith		Affirmative	N/A
3	MEAG Power	Roger Brand	Rebika Yitna	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Benjamin Widder		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Amy Wesselkamper		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Christopher Murphy		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	N/A
3	Santee Cooper	Vicky Budreau		Affirmative	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Negative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Ryan Walter		Affirmative	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Arkansas Electric Cooperative Corporation	Jenni Sudduth		Abstain	N/A
4	Austin Energy	Tony Hua		Affirmative	N/A
4	Buckeye Power, Inc.	Jason Procuniar	Ryan Strom	Negative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Negative	N/A
4	DTE Energy	Patricia Ireland		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Negative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	AES - AES Corporation	Ruchi Shah		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	N/A
5	Buckeye Power, Inc.	Kevin Zemanek	Ryan Strom	Negative	N/A
5	Calpine Corporation	Whitney Wallace		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar	Marie Potter	Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Decatur Energy Center LLC	Megan Melham		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Greybeard Compliance Services, LLC	Mike Gabriel		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Negative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	LS Power Development, LLC	C. A. Campbell		None	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	NextEra Energy	Richard Vendetti		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Omaha Public Power District	Kayleigh Wilkerson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		Affirmative	N/A
5	Pacific Gas and Electric Company	Frank Lee	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pattern Operators LP	George E Brown		None	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Sacramento Municipal Utility District	Ryder Couch	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	N/A
5	Santee Cooper	Carey Salisbury		Affirmative	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tri-State G and T Association, Inc.	Sergio Banuelos		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Abstain	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Abstain	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco	Marie Potter	Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Negative	N/A
6	Invenergy LLC	Colin Chilcoat		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Laura Wu		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	N/A
6	Santee Cooper	Marty Watson		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Negative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Western Area Power Administration	Jennifer Neville		Negative	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 254 of 254 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Exhibit G

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Drafting Team Roster

Project 2023-03 Internal Network Security Monitoring (INSM)

	Name	Entity
Chair	Thad Ness	NextEra Energy
Vice Chair	Valerie Ney	FirstEnergy Corporation
Members	Joseph Jimenez	Duke Energy
	Dan Toth	American Transmission Company, LLC
	Mark Johnson-Barbier	Salt River Project
	Joseph Bradley	Ameren
	Erin Wilson	New Brunswick Power
	Robert Rinish	PPL Electric Utilities
	Aaron Williams	Southern Company
	Eric Rupp	Great River Energy
	Alan Kloster	Evergy, Inc.
	Darcy Guenette	Ontario Power Generation
	Tim McDonald	PG&E
	David Crim	MISO
PMOS Liaison	Ruida Shu	NPCC
NERC Staff	Laura Anderson – Senior Standards Developer	North American Electric Reliability Corporation

	Name	Entity
	Linda Jenkins – Senior Standards Development Administrator	North American Electric Reliability Corporation
	Sarah Crawford – Counsel, Legal & Regulatory	North American Electric Reliability Corporation