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)](https://sbs.nerc.net/) to submit comments on **Project 2023-03 INSM/CIP-015-1 – Internal Network Security Monitoring** by **8 p.m. Eastern, Monday, March 18, 2024.
m. Eastern, Thursday, August 20, 2015**

Additional information is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project-2023-03-INSM.aspx). 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]](#footnote-2) 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]](#footnote-3) 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 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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

1. 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:

1. 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:

1. Please provide any additional comments for the DT to consider, if desired.

Comments:

1. *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023). [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)