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, Wednesday, April 17, 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](mailto:Laura.anderson@nerc.net), 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 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.

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]](#footnote-4)
* 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

## 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:

1. 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:

1. 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:

1. 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:

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: (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. [↑](#footnote-ref-3)
3. In a [Letter Order](http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter%20Order%20Approving%20Revised%20SPS%20Definition.pdf) 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). [↑](#footnote-ref-4)