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-007-X Cyber Security – Systems Security Management** by **8 p.m. Eastern, Wednesday, January 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, 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**

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.

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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. Please provide any additional comments for the SDT 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)