Unofficial Comment Form

Project 2025-02 Internal Network Security Monitoring (INSM) Standard Revision

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on the **Project 2025-02 Internal Network Security Monitoring Standard Revision** Standard Authorization Request (SAR)by **8 p.m. Eastern, Friday, August 15, 2025.**

Additional information is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project202502InternalNetworkSecurityMonitoringStandardRevision.aspx). If you have questions, contact Senior Standards Developer, [Laura Anderson](mailto:laura.anderson@nerc.net) (via email), or at 404-782-1870.

## Background Information

On June 26, 2025, the Federal Energy Regulatory Commission (FERC) approved proposed Reliability Standard CIP-015-1 and issued Order No. 907[[1]](#footnote-1) directing NERC to develop certain modifications to Reliability Standard CIP-015-1 to extend Internal Network Security Monitoring (INSM) to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) outside of the Electronic Security Perimeter (ESP). FERC Order No. 907 also provides clarity around the term CIP-networked environment as it is used in Reliability Standard CIP-015-1. FERC directed NERC to submit these revisions for approval within 12 months of the effective date of the final rule, September 1, 2026.

Although proposed Reliability Standard CIP-015-1 was approved, FERC determined that a reliability and security gap remained because CIP-015-1 does not require implementation of INSM for the entire CIP-networked environment. While the CIP Reliability Standards require monitoring of the ESP 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 include EACMS and PACS outside of the ESP. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack.

**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:

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

Comments:

1. *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security --* *Internal Network Security Monitoring*, Order No. 907, 191 FERC ¶ 61,224 (June 26, 2025). [↑](#footnote-ref-1)