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.