NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-03 INSM

Industry Webinar
March 6, 2024

RELIABILITY | RESILIENCE | SECURITY




Administrative

- North American Electric Reliability Corporation (NERC) Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

Agenda

- Drafting Team (DT)
- Background
- Key Changes from initial comment and ballot period
- Comparison of initial comment and ballot period vs. additional comment and ballot period
- CIP-015-1 Requirements and Requirement Parts
- Contact Information
- Q&A

Standard Drafting Team

Name	Entity
Thad Ness, Chair	NextEra Energy
Valerie Ney, Vice Chair	FirstEnergy Corporation
Joseph Jimenez	Duke Energy
Dan Toth	American Transmission Company, LLC
Mark Johnson-Barbier	Salt River Project
Erin Wilson	New Brunswick Power
Robert Rinish	PPL Electric Utilities
Aaron Williams	Southern Company
Eric Rupp	Great River Energy
Alan Kloster	Evergy, Inc.
Darcy Guenette	Ontario Power Generation
Tim McDonald	PG&E
David Crim	MISO

Background

- Internal Network Security Monitoring (INSM) permits entities to monitor traffic within a trusted zone (e.g., Electronic Security Perimeter (ESP)) to detect intrusions or malicious activity.

- January 19, 2023 – FERC Order No. 887 directed NERC to:
  - Develop requirements within CIP Reliability Standards for INSM
    - High-impact Bulk Electric System (BES) Cyber Systems
    - Medium impact BES Cyber Systems with External Routable Connectivity (ERC)
  - FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Background

- Based on industry comments received, the DT concluded that INSM requirements do not fit clearly into any existing standard and would be best implemented as a new standalone standard: CIP-015-1.

Background

- The initial posting included EACMS and PACS devices outside of the ESP within the applicability section as part of the CIP-Networked Environment.

- Based upon a review of the comments, the Project 2023-03 DT noted that the term CIP-Networked Environment is not a defined term and determined that the record does not support inclusion of EACMS and PACS outside of the ESP.

- Reliability Standard CIP-015-1 only includes networks within each ESP of high and medium impact (with ERC) BES Cyber Systems in its applicability scope.

Key Changes from Initial Posting

- Developed new proposed Reliability Standard CIP-015-1.
  - Initial posting included draft Requirement R6 in CIP-007-X.
  - Switched from CIP table format to traditional Requirement/Measure format.
  - Focus is on networks within each ESP and not the BES Cyber System.
- Scope of networks now only include those within each ESP
  - Initial posting included select EACMS and PACS outside the ESP.
- Data protection and retention have been moved into separate requirements.
- Included CIP Exceptional Circumstance language in the data protection and retention requirements.

Maintain objective-based requirements to ensure flexibility and future change

Comparison of Initial Posting vs. Additional Posting 1

Initial Posting (CIP-007-X, Requirement R6)	Additional Posting 1 (CIP-015-1)
Applicable Systems High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs … Scope is the networks within ESPs

Comparison of Initial Posting vs. Additional Posting 1

Initial Posting (CIP-007-X, Requirement R6)	Additional Posting 1 (CIP-015-1)
R6. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-X Table Requirement R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls.	R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. Provided additional clarity on the parent requirement

Comparison of Initial Posting vs. Additional Posting 1

Initial Posting (CIP-007-X, Requirement R6)	Additional Posting 1 (CIP-015-1)
Requirement R6, Part 6.1 Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Requirement R1, Part 1.1. Identify network data collection locations and methods, based on the network security risk(s), to monitor network activity including connections, devices, and network communications. Included “based on network security risk” Remove “100 percent coverage is not required”

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comparison of Initial Posting v. Additional Posting 1

Initial Posting (CIP-007-X, Requirement R6)	Additional Posting 1 (CIP-015-1)
Requirement R6, Part 6.2 Log collected data regarding network communications at the network locations identified in Part 6.1.	Removed "log" requirement.
Requirement R6, Part 6.3 Evaluate the collected data to document the expected network communication baseline.	Requirement R1, Part 1.2. Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1.
Requirement R6, Part 6.4 Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Consolidated requirements. No longer formally requires a baseline.
Requirement R6, Part 6.5 One or more process(es) to evaluate anomalous activity identified in Requirement R6, Part 6.4 to determine appropriate action.	Requirement R1, Part 1.3. Implement one or more method(s) to evaluate activity Removed "anomalous" since it is referenced in 1.2 above.

Comparison of Initial Posting v. Additional Posting 1

Initial Posting (CIP-007-X, Requirement R6)	Additional Posting (CIP-015-1)
Requirement R6, Part R6.6 Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Requirement R3, Part R3. Responsible Entity shall implement one or more documented process(es) 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, except during CIP Exceptional Separate requirement and added CEC
Requirement R6, Part R6.7 One or more process(es) to protect the data collected in Requirement R6, Part R6.2 to mitigate the risks of deletion or modification by an adversary	Requirement R2, Part R2. Responsible Entity shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Separate requirement and added CEC

CIP-015-1, Requirement R1

- CIP-015-1, Requirement R1.
  - R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*
    - [Requirement Parts included in subsequent pages]
  - M1. Evidence must include each of the applicable documented process(es) that collectively include each of the applicable requirement parts in Requirement R1 and additional evidence to demonstrate implementation as described in the measure parts. Examples of evidence may include, but are not limited to, one or more of the following for each Part:

CIP-015-1, Requirement R1, Part R1.1

- Requirement R1, Part R1.1
  - Identify network data collection locations and methods, based on the network security risk(s), to monitor network activity including connections, devices, and network communications.
- Corresponding Measure M1, Part M1.1
  - Architecture documents or other documents detailing data collection methods; or
  - Documented rationale on how network locations were selected or excluded for data collection.
- Risk-based instead of prescriptive
  - Too many different network architectures and edge cases; and
  - Responsible Entities will have to document their data collection design and then defend the decisions on where and how they collect data for INSM.

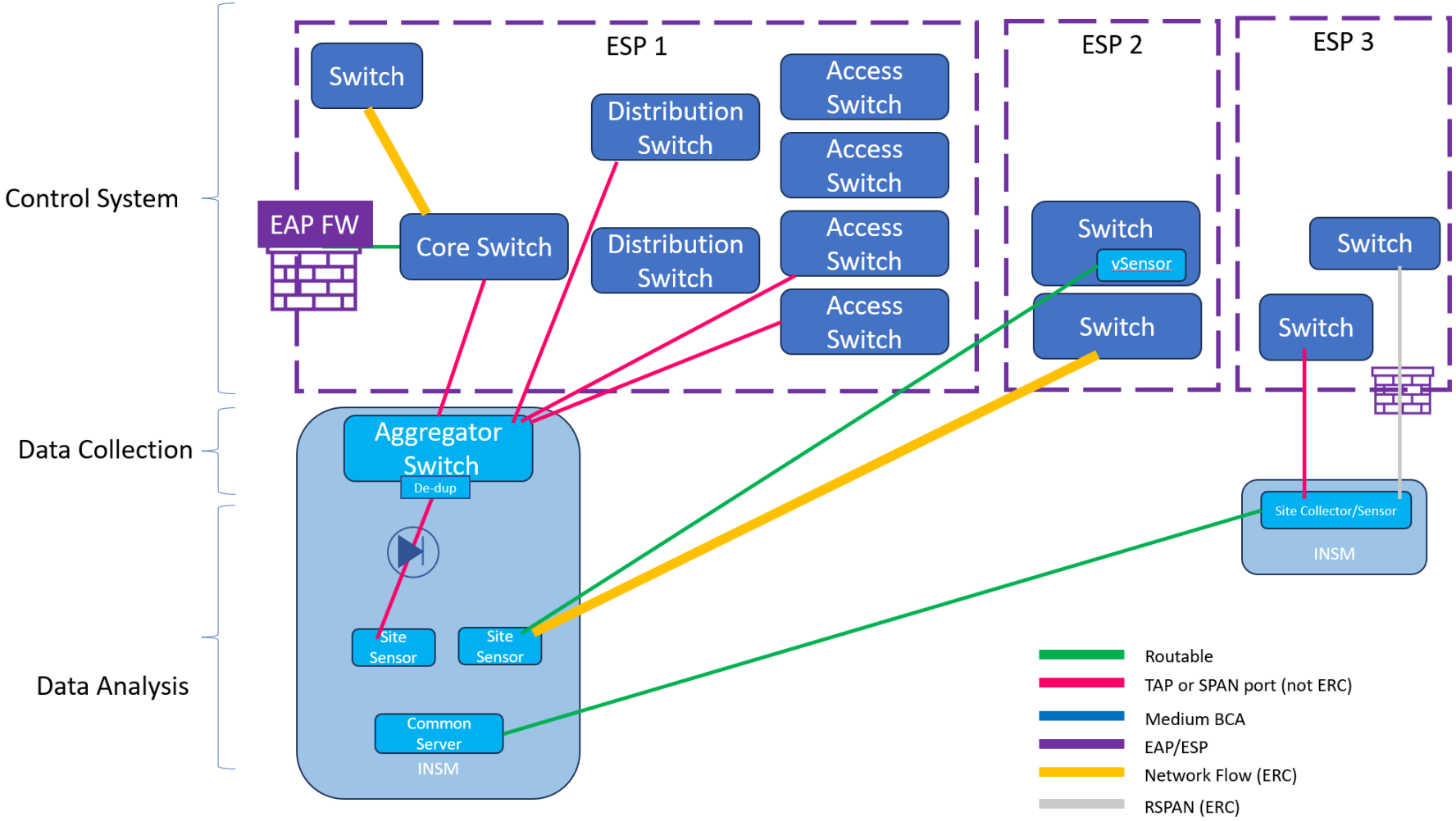
CIP-015-1, Requirement R1, Part R1.1

> *"He who defends everything, defends nothing."*
>
> *Attributed to Fredrick the Great*

- Collection – Balance
  - Identify convergence locations
  - Start collection of higher value data
  - Tune/add/remove data collection locations over time
  - Layer 2 and Layer 3 network traffic collection as needed
  - Balance with other capabilities (SIEM/Endpoint/EDR)
- Some Level of INSM Network Collection
  - Full PCAP (TAP, SPAN)
  - Remote collection (RSPAN, Net Flow)
  - SDN logs or others as described in the Technical Rationale

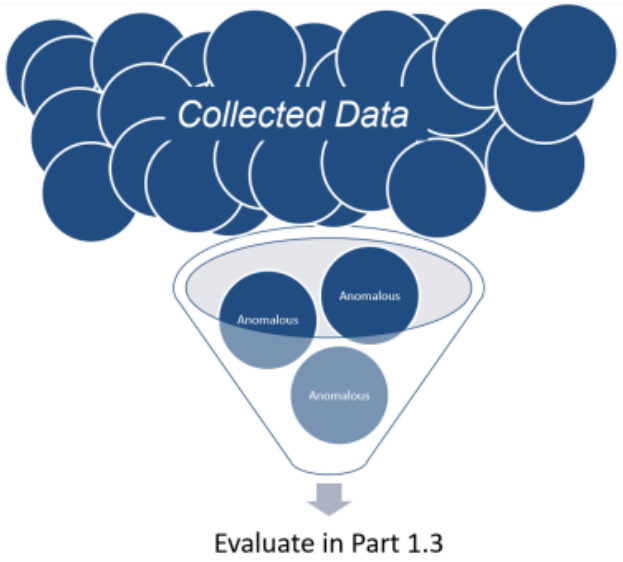
CIP-015-1, Requirement R1, Part R1.1

Reference Architecture



CIP-015-1, Requirement R1, Part R1.2

- Requirement R1, Part 1.2
  - Implement one or more method(s) to detect anomalous network activity using the data collected at locations identified in Part 1.1.
- Corresponding Measure M1, Part M1.2
  - Detection events;
  - Configuration settings of INSM monitoring systems; or
  - Documentation of a baseline used to monitor against unauthorized network activity.
- Allows Flexibility
  - Provides for different technologies to be used.
  - Reference to baseline is one possible measure.
  - Anomalous network activity could include authorized or unauthorized network activity.



CIP-015-1, Requirement R1, Part R1.3

- Requirement R1, Part R1.3
  - Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action.
- Corresponding Measure M1, Part 1.3
  - Documentation of method(s) used to evaluate anomalous activity;
  - Documentation of responses to detected anomalies, etc.; or
  - Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).
- Leverage detections from Requirement R1, Part R1.2
  - Responsible Entities should document what they will do to determine if anomalous traffic identified in R1.2 requires additional investigation, escalation, INSM tuning if it is a false positive, or other action to be taken.
  - Does not necessarily indicate CIP-008 escalation.

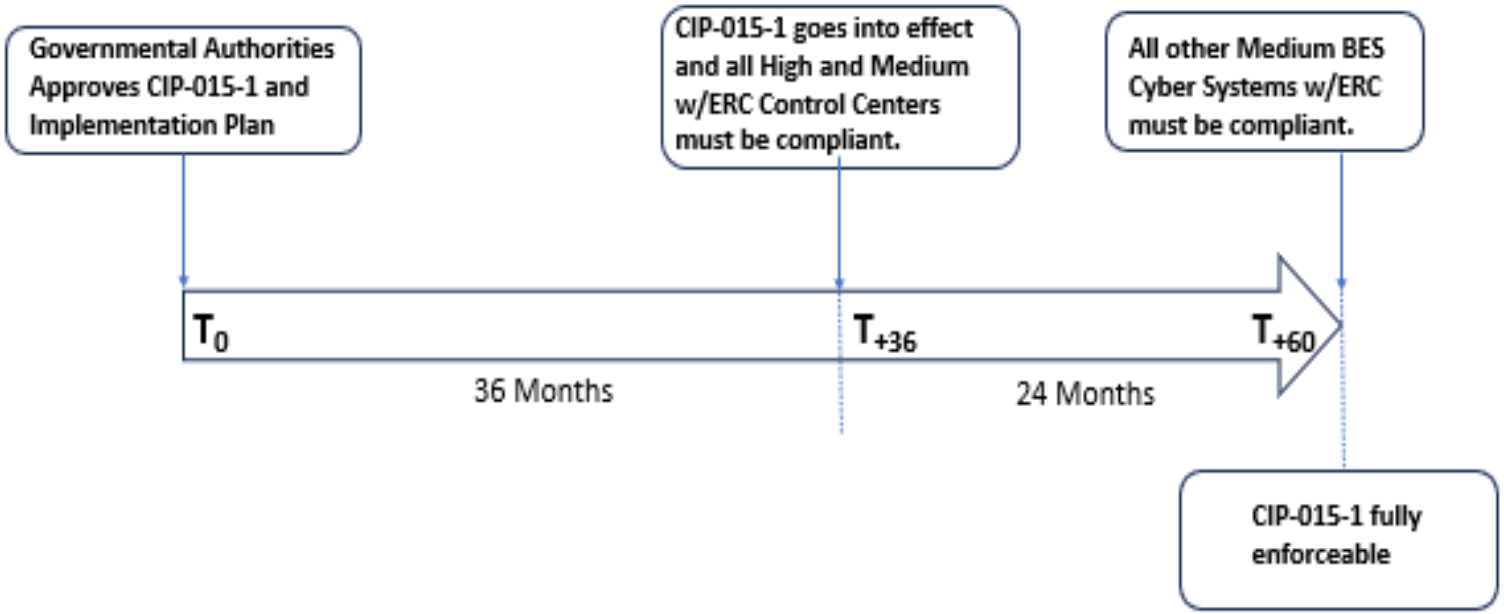
CIP-015-1, Requirement R2

- Requirement R2:
  - Responsible Entity shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*
- Corresponding Measure M2:
  - Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of unauthorized deletion or modification.
- From Order No. 887:
  - "Minimize the likelihood of an attacker removing evidence of TTPs from compromised devices."
  - Controls for protecting BCSI are sufficient.

CIP-015-1, Requirement R3

- Requirement R3:
  - Responsible Entity shall implement one or more documented process(es) 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, except during CIP Exceptional Circumstances. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*
- Corresponding Measure M3:
  - Examples of evidence may include, but are not limited to, documentation of the data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to perform the analysis of actionable anomalous activity
- Responsible Entities determine what data to retain and for how long.
- Metadata is a record of past traffic or a summarization of that traffic.

Implementation Plan



Additional Posting 1

- February 27, 2024 through 8:00 p.m. Eastern March 18, 2024
  - Although NERC's system will reflect the posting as an initial ballot, this posting is an additional ballot for Project 2023-03.
  - Based on comments received, the DT has created a new proposed Reliability Standard CIP-015-1, rather than propose revisions to CIP-007.
  - As a result, there will be no changes to CIP-007 and it will revert to the currently-enforced version.

Questions & Answers

- Informal Discussion
  - Via the Questions and Answers feature.
  - Respond to stakeholder questions.

- Other
  - Some questions may require future DT consideration.
  - Please reference slide number, standard section, etc., if applicable.
  - DT will address as many questions as possible.
  - Webinar and chat comments are not a part of the official project record.
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the DT.

Project 2023-03 INSM Contact Information

- Point of Contact
  - Laura Anderson, Senior Standards Developer
    - laura.anderson@nerc.net or call 404-782-1870
- Webinar Slides and Recording Posting
  - Within 24-72 hours of Webinar completion.
  - Link will be available in the Standards, Compliance, and Enforcement Bulletin.

Questions and Answers