NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-03 INSM
Industry Webinar

April 10, 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
- Ballot Results
- General Changes
- CIP-015-1 Requirements and Requirement Parts
- Implementation Plan
- FAQ Document
- Technical Rationale Document
- 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.

Ballot Results

Project 2023-03 Internal Network Security Monitoring

Standard Name	Initial Ballot	Additional Ballot	Score Change (Initial Ballot to Additional Ballot)
CIP-007-X R6	15.42%	--	--
CIP-015-1	--	48.52%	+33.10%
Non-Binding Poll	11.98%	47.54%	+35.56%
Implementation Plan	44.89%	66.71%	+21.82%

CIP-015 Additional Posting 2 – General Changes

- Generator Owner (GO) added to Functional Entities.
  - Inadvertent omission shifting from modifications in CIP-007 to CIP-015
- References to Special Protection System (SPS) changed to Remedial Action Scheme (RAS).

CIP-015 Additional Posting 2

R1. Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts.

- Concept of "within ESP" changed to "protected by."
  - "Within" doesn't always exist in modern networks (e.g., zero trust).
- "Unauthorized" removed from Requirement R1.
  - Implies other communications are formally authorized.
- "Increase the probability of" changed to "provide methods for."
  - Phrase was subjective.

CIP-015 Additional Posting 2

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

- Network data collection "locations" changed to "feeds."
  - Received concerns about having to document physical locations.
- Altered Measure M1 language to give entities the ability to defend why data collection feeds were **selected** rather than having to defend why feeds were **excluded.**

CIP-015 Additional Posting 2

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

- The DT declined to add “technical capabilities” exception to Requirement R1. Part 1.1.
  - Concerns about creating a loophole.
- “Based on network security risks” changed to “using a risk-based rationale.”

CIP-015 Additional Posting 2

R2. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

- Added "**and data retained in support of Requirement R3**" to clarify that retained INSM data needs to be protected as well.
- Moved the CIP Exceptional Circumstances language to clarify that it applied to the Requirement R2 process.

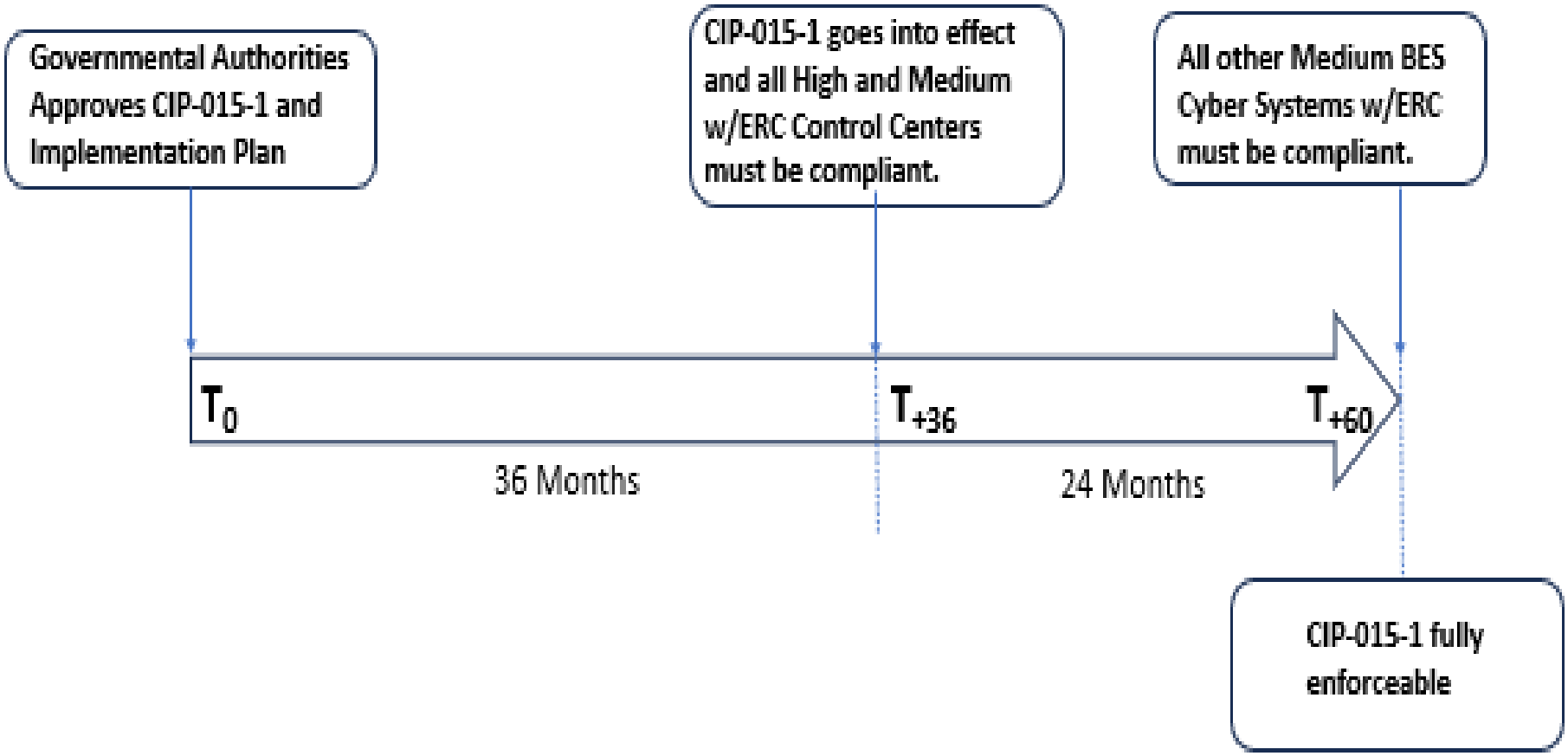
CIP-015 Additional Posting 2

R3. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- Large number of comments / concerns around data retention requirements and time periods.
- "at a minimum until the action is complete"
  - Setting a minimum bound on data retention
- "Note:…"
  - Ensuring there is an explicit statement about not needing to retain data that is not relevant to anomalous network activity detected

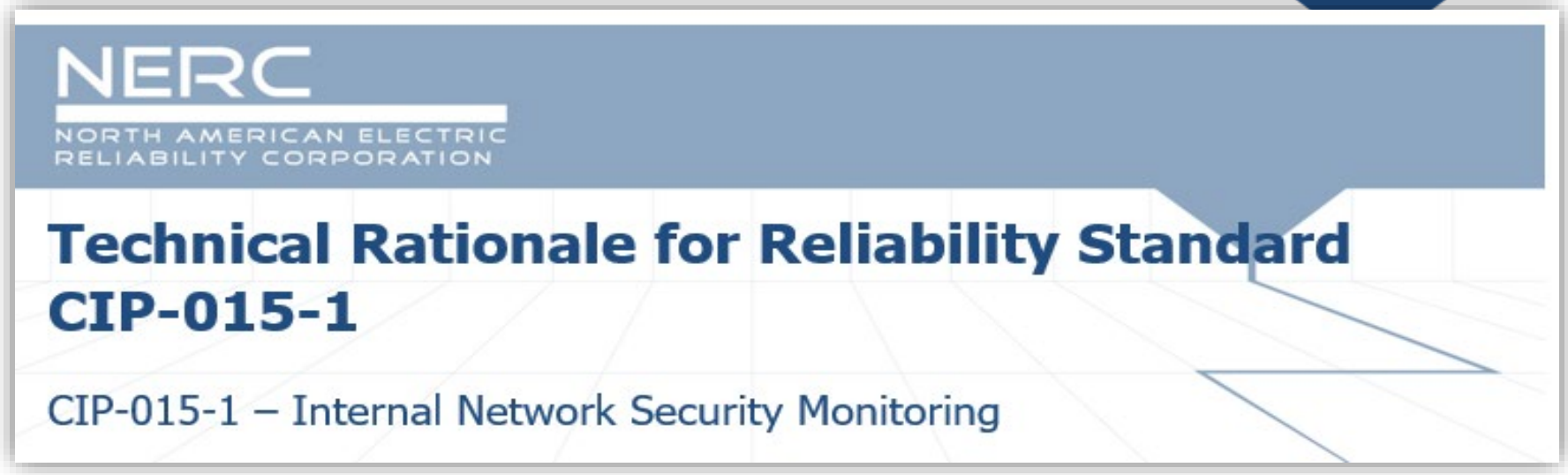
Implementation Plan



CIP-015 Additional Posting 2 – FAQ

- Answers 10 common questions the DT has received over the course of the project.

CIP-015 Additional Posting 2 – Technical Rationale



- Detailed documentation about INSM theory and capabilities.
- Documents the reasoning behind the language of the requirements, and the risks that they are trying to address.

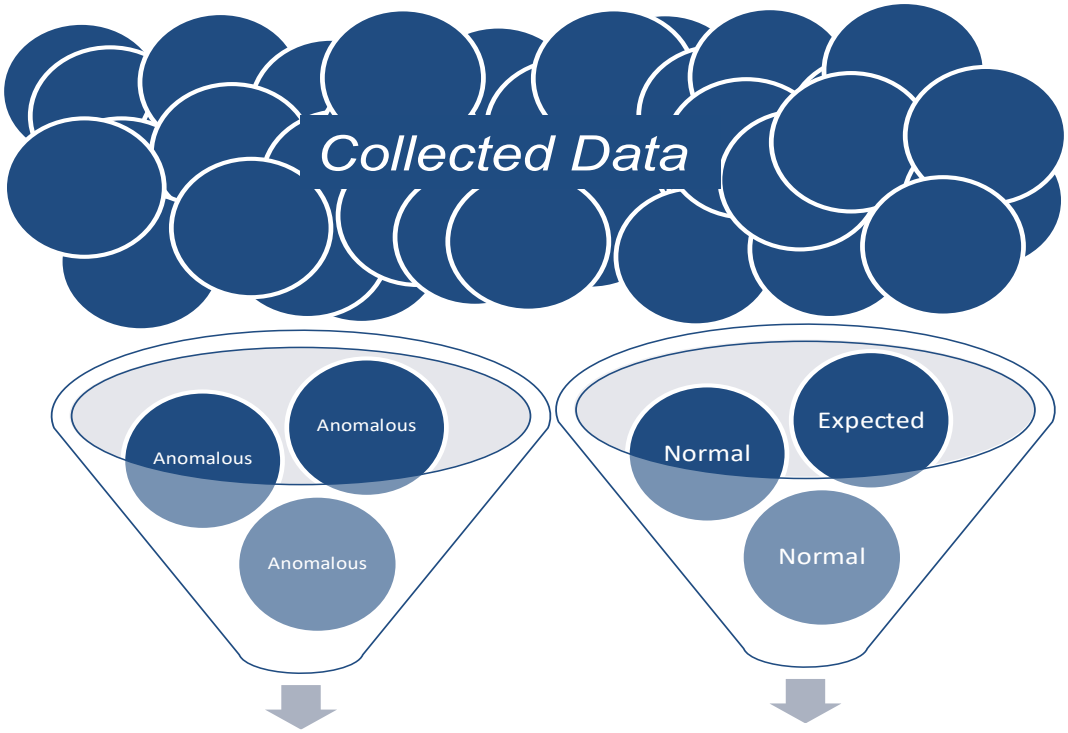
CIP-015 Additional Posting 2 – Technical Rationale

R1.1 requires entities to implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

R1.2 requires entities to detect anomalous network activity.

R2 requires entities to protect the data collected from unauthorized deletion or modification.

R3 requires entities to retain the data related to anomalous activity for analysis in 1.3 and potentially to meet CIP-008 requirements if the anomalous activity is associated with a cybersecurity incident or attempt to compromise.



Evaluate in Part 1.3

R1.2 requires entities to detect anomalous network activity.

R3 does not require retention of normal and expected data

Next Steps

- April 5, 2024 – 13-day additional comment period with 5-day ballot
- April 17, 2024 – Ballot closes at 8:00 p.m. Eastern
- April 19, 2024 – DT meeting
- April 22, 2024 – DT meeting

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