NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Meeting Notes
Project 2023-03 Internal Network Security Monitoring

March 21, 2024

Conference Call

Administrative

1. **Introductions**
   The meeting was brought to order by the Chair at 1:30 p.m. Eastern on Thursday, March 21, 2024.

2. **Determination of Quorum**
   The rule for NERC Drafting Team states that a quorum requires two-thirds of the voting members of the DT. Quorum was achieved as 11 of 14 total members were present.

3. **NERC Antitrust Compliance Guidelines and Public Announcement**
   NERC Antitrust Compliance Guidelines and public announcement were reviewed by Laura Anderson. There were no questions raised.

Agenda

1. **Discussion**

   a. Project update from additional ballot:

   - Thad Ness, Chair and Valerie Ney, Vice Chair, presented the project to the Standards Committee at their March 2024 meeting.
     - Valerie Ney, Vice Chair, presented to the DT and observers the same presentation provided to the Standards Committee.
       - Industry supported (100% supportive comments) removal of EACMS and PACS outside of the ESP.
       - Overwhelmingly positive response (97% supportive comments) of creating a new Reliability Standard, CIP-015-1, and not modifying CIP-007.

   b. Comments received:

   - Anomalous:
     - Difficult to be prescriptive because the DT would have no idea what might be anomalous in a Responsible Entity's networks.
     - A suggestion was raised to identify what anomalous activity is not.
     - Keeping data long enough to make a judgement on the anomalous traffic.
     - Industry provided comments that the DT considered in making revisions.
       - Comments suggested that cost effectiveness would be tied to the data retention and logging.
     - Concern with storing at substations, so the DT needs to revise to provide clarity on what types of data needs to be stored.
   - Many commenters suggested to remove "unauthorized" from Requirement R1 since it is not mentioned elsewhere and there is some overlap with CIP-008; the DT agreed.
     - Leaving "unauthorized" in would imply processing that could be extremely difficult to automate.
   - The DT will have to balance Requirement R1 between risk-based and prescriptive.
   - "Data collection methods" was previously discussed and the DT decided to change this to "network data feeds."
     - The DT defined data feeds as a combination of locations and methods for collection in the Technical Rationale document.
   - Measure M1 was updated to better align with Requirement R1 and its Parts, for consistency, and to align with similar language in the CIP family of standards.
   - Requirements R2 and R3:

- CIP-011 protects BCSI and the goal that was intended by the Order was to secure the TTP. As written, does this impose a mitigation of risk to the integrity of the TTP?
- Requirement R2 is to protect and Requirement R3 is to retain.
- The following note was added following Requirement R3:
    - “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.”

- Requirement R3:
    - Revised Requirement R3, removing “with sufficient detail and duration.”
        - Entities can choose to store more for threat hunting.
        - Retain long enough to do the analysis.
        - Entities would likely choose to capture PCAP based on alerts.
        - The DT could make that part of the Measure as well.
        - Being specific would cause problems with some of the tools.
        - Entities know their operation better than anyone else:
- How many alerts on average that could change over time.

c. Outreach opportunities/assignments

- Thad Ness, Chair, to present at NATF during their panel.
- Thad Ness, Chair and Valerie Ney, Vice Chair, presented the project to the Standards Committee at their March 2024 meeting.
    - Valerie Ney, Vice Chair, presented to the DT and observers the same presentation provided to the Standards Committee.
        - Industry supported (100% supportive comments) removal of EACMS and PACS outside of the ESP.
        - Overwhelmingly positive response (97% supportive comments) of creating a new Reliability Standard, CIP-015-1, and not modifying CIP-007.
- NAGF April 2024
- The DT members will be socializing revisions as opportunities arise.

d. FAQ creation for Additional Posting:

- Alan will be drafting a FAQ document.

2. Action Item Review

a. Consideration of Comments:

- DT to review, provide inputs and edits.

b. Technical Rationale:

- Mark Johnson-Barbier, Member, to update as revisions are made to proposed Reliability Standard CIP-015-1 and as comments received related to Technical Rationale are vetted.

c. Proposed Reliability Standard CIP-015-1:

- DT to continue making revisions.

d. Implementation Plan:

- DT to review as revisions are made to proposed Reliability Standard CIP-015-1.

e. VRF/VSL Justification Document:

- DT to review as revisions are made to proposed Reliability Standard CIP-015-1.

f. FAQ Document:

- Alan Kloster, Member, to draft FAQ document.

3. Future meeting(s)

a. March 22, 2024 – WebEx

b. March 25, 2024 – WebEx

c. March 26, 2024 – WebEx

4. Adjourn

The meeting adjourned at 2:51 p.m. Eastern on March 21, 2024.

Attendance

Name	Company	Member/ Observer	In-person (Y/N)	Conference Call (Y/N)
Thad Ness, Chair	NextEra Energy	Member	N	Y
Valerie Ney, Vice Chair	FirstEnergy Corporation	Member	N	Y
Joseph Jimenez	Duke Energy	Member	N	N
Dan Toth	ATC	Member	N	Y
Mark Johnson-Barbier	Salt River Project	Member	N	Y
Joseph Bradley	Ameren	Member	N	Y
Erin Wilson	New Brunswick Power	Member	N	Y
Robert Rinish	PPL Electric Utilities	Member	N	N
Aaron Williams	Southern Company	Member	N	Y
Eric Rupp	Great River Energy	Member	N	N
Alan Kloster	Evergy, Inc.	Member	N	Y
Darcy Guenette	Ontario Power Generation	Member	N	Y
Tim McDonald	PG&E	Member	N	Y
David Crim	MISO	Member	N	Y
Ruida Shu, PMOS Liaison	NPCC	PMOS	N	Y
Laura Anderson, NERC staff	NERC	NERC Staff	N	Y
Sarah Crawford, NERC Legal	NERC	NERC Staff	N	Y