NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2022-05 Modifications to CIP-008 Reporting Threshold Drafting Team

February 24, 2025 | 2:00 – 4:00 p.m. Eastern

Review NERC Antitrust Compliance Guidelines and Public Announcement

Jason Snider, NERC staff, called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice.

Roll Call and Determination of Quorum

A team roll call was taken and quorum was determined. The member attendance sheet is attached as attachment 1.

Opening Remarks

T. Hall, chair, welcomed the group and gave an overview of the group's goal for the day – to review potential attachment 1 tables, similar to the one used in EOP-004, to better align the group's work with the goals laid out in the SAR.

Project updates

During the previous teleconference, members were asked to draft potential tables to review. The group reviewed two drafts (first rows provided here as an example). The first draft was by S. Klauminzer:

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Malware incidents (e.g. Ransomware, Fileless malware, Botnet activity)		• When affecting an applicable system – Report per R4 Part 4.2.1 • When affecting an adjacent system, with the target of an applicable system – Report per R4 Part 4.2.2

The group discussed attack types, intel received from government entities, ISACs, and peers, as well as types of intel to share back out if/when discovered internally.

Next the group reviewed a draft by S. Koller:

Condition Description (Event of Interest)	Target (Applicable System[1])	Incident Type and Threshold for Reporting
Reconnaissance activity	BCS	Cyber Security Incident of the EACMS, and Attempted Cyber Security Incident against the BCS
	EACMS	Attempted Cyber Security Incident against the EACMS
	PCA	Cyber Security Incident of the EACMS, and Attempted Cyber Security Incident against the BCS
	PACS	NA

S. Koller noted that the columns were changed to include conditions, target applicable systems, and incident types and reporting thresholds.

The group discussed the merits of the two options, eventually agreeing that the solution was likely a combination of the two. Time was also spent reviewing the scope of the definitions around TCAs and removable media in relation to applicable systems.

The remaining time was spent discussing what was needed to provide clarity for next steps:

- J. Rowe to present a high-level example of an audit against the current draft language
- Investigate leveraging the Mitre Attack ICS framework or the CIPC to build out the EOP-004 attachment with reportability criteria.
- The need for extensive outreach to inform industry of the proposed changes and the rationale behind them.
- Inviting E-IASC to participate to ensure the end result of the proposed changes is beneficial.

Action Items

- Team to review proposed tables and bring other potential approaches for the next meeting.
- J. Rowe to present a high-level example of an audit against the current draft
- J. Snider to identify E-IASC contact for the group to discuss Attachment 1 table options during a future meeting.

Parking lot

- Definitions
- Feedback on use of “may” in definitions
- Definitions – what is being impacted?
- Coordination with DOE 417 (updating external forms)

[1] Applicable Systems refer to High and Medium impact BCS and their associated EACMS, PACS, and PCA.

- Applicable systems
- Include specific language in each primary requirement
- Requirement language
- Technical Rationale
- Implementation Guidance
- Updating slide deck

Attachment 1

Name	Entity	2/24/25
Tony Hall	LG&E and KU Energy	Y
Sharon Koller	American Transmission Company, LLC	Y
Marc Child	Great River Energy	N
Bryan Yoch	Ameren	Y
Joshua Rowe	WECC	Y
Brent Howell	Duke Energy	N
Scott Klauminzer	Tacoma Public Utilities	Y
Lawrence Good	Bonneville Power Administration	y