NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

March 10, 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. As quorum had not been reached, the group would focus on reviewing possible paths forward with the goal of having a strawman draft to review on the group's next call.

Project updates

T. Hall began by sharing a recommendation received since the previous call for the team to review NIST's Computer Security Incident Handling Guide (SP 800-61 Rev. 2)

In NIST's Computer Security Incident Handling Guide (SP 800-61 Rev. 2), the term "attempted compromise" typically falls under security incidents and can include activities such as:

- **Scanning and Probing:** Reconnaissance activities that aim to discover vulnerabilities.
- **Brute Force Attacks/Excessive Failed Authentication Attempts:** Unsuccessful attempts to guess credentials or encryption keys.
- **Phishing Attempts:** Malicious emails or messages intended to deceive users into revealing credentials.
- **Exploitation Attempts:** Attempts to exploit vulnerabilities in systems, software, or networks that are blocked or unsuccessful.
- **Denial-of-Service (DoS) Attempts:** Unsuccessful efforts to disrupt availability.
- **Ransomware:** malicious software (malware) that encrypts or locks a victim's data or entire system, rendering it inaccessible until a ransom is paid.

- **Data Exfiltration Attempts**: potential insider threats malicious or accidental.

There was general agreement with this approach, though it was noted that the language around phishing may need to be adjusted to something referencing targeted phishing.

The group also reviewed an older document, Security Guidance for electric sector threat and incident reporting. Though the team felt the document was worth reviewing, those on the call felt that drafting a Table similar to EOP-004 influenced by the NIST 800-61 language was the more favorable choice. T. Hall suggested that language be drafted for the group to review on the next call. In addition to this, he suggested that a draft be created focusing on including language in the measurements. During the next call, the group could review the two documents and determine the best path forward. Additionally, he suggested the group begin drafting a technical rationale document to include in the upcoming informal posting.

Action Items

- T. Hall to draft strawman – table version
- M. Child to draft strawman – measurements version
- T. Hall to begin drafting Technical Rationale, focusing on R1. L. Good and B. Yoch to assist with review.
- J. Snider to identify E-ISAC 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)
- Applicable systems
- Include specific language in each primary requirement
- Requirement language
- Technical Rationale
- Implementation Guidance
- Updating slide deck

Attachment 1

Name	Entity	3/10/25
Tony Hall	LG&E and KU Energy	Y
Sharon Koller	American Transmission Company, LLC	N
Marc Child	Great River Energy	Y
Bryan Yoch	Ameren	Y
Joshua Rowe	WECC	Y
Brent Howell	Duke Energy	N
Scott Klauminzer	Tacoma Public Utilities	N
Lawrence Good	Bonneville Power Administration	Y