NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

May 12, 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 goals for the call – time would be given to both E-ISAC and NERC compliance staff to provide feedback on the potential paths the group had identified, and then determining which approach the group wanted to proceed with.

Project updates – E-ISAC feedback

M. Duncan (E-ISAC) presented to the group, providing information on the reporting that E-ISAC receives, how it uses the data, and what type of information it is looking for. He noted that there is a shift occurring, moving from being indicator-based to focusing on the actionable intel behind potential attacks. L. Gattone (E-ISAC) explained that the E-ISAC encourages entities to use incident reporting templates to fully capture relevant information, and shared some questions that are used to follow up on items submitted to them:

- Is the impacted system covered under CIP-008, and can you share the type of equipment impacted?
- Do you have any assessment on the potential motive or desired outcome of the observed behavior?
- Do you have any assessment on potential motive(s), suspect(s), or why the site was targeted? Are you aware of any previous cybersecurity threats to the site?
- Has law enforcement been contacted? If so, can you share any insights from your interaction with them?
- Do you have additional indicators to provide beyond what was posted/shared?

Project updates – NERC Compliance feedback

L. Ratliff (NERC Compliance) provided feedback on the potential paths the group had discussed. He asked the group to focus on how potential language changes would meet the intent of the previous FERC order. The group spent time discussing how to determine what an attempt to compromise was, how to determine

intent, and how these factored into reportability. It was noted that some events were not being categorized as compromises because they did not impact the BES directly. L. Ratliff suggested the group review FERC Order 848 which drove the previous revisions to CIP-008.

Project updates – next steps

The drafting team agreed that adding "which at a minimum include events, alerts, or alarms detected by one or more requirement parts in CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, or CIP-015" to 1.2.1 of the current standard would not address the concerns, and chose to resume work on the earlier draft. S. Koller suggested the group may need to define or at least add clarity in the Technical Rationale around what was considered a "Compromise" and what constituted an "Attempt to Compromise".
Sharon: take an approach of "evaluating" or requiring a process rather than criteria?

Action Item

- Drafting team to consider "compromise" and "attempt to compromise" and be prepared to discuss on next teleconference.

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	5/12/25
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	Y
Scott Klauminzer	Tacoma Public Utilities	Y
Lawrence Good	Bonneville Power Administration	Y