

Meeting Notes

Project 2022-05 Modifications to CIP-008

Reporting Threshold

Drafting Team

May 27, 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.

Project updates – review of E-ISAC and NERC compliance feedback

The drafting team spent time reviewing the feedback received during the previous teleconference, focusing largely on the concern raised by NERC compliance that attempts were not being reported due to judgements such as no effect on the BPS / operations, or the duration of time. The group agreed that strengthening the evaluation or analysis process was a possible step in the right direction. This led to discussion around keeping the evaluation process broad enough (instead of listing specific activities) to cover new versions of attacks as well as new technologies. S. Klauminzer noted that the criteria for an attempt to compromise seemed to be focused not on the type of event itself, but on the reporting decision. L. Good asked if the language was being drafted around the desired outcome instead of the actual events. S. Klauminzer added that the group may have unintentionally changed the threshold for reporting by changing the definition of a Cyber Security Incident, and the group considered the need to revise the proposed definitions, or adding additional terms, such as “Cyber Attach” to avoid further revisions in the standard itself. The team next discussed how to validate “attempt to compromise” criteria -- an actual compromise has impact, but an attempt (something stopped) is at times unable to be addressed through methodology. S. Klauminzer pointed out that the group should consider the original [FERC order 848](#) phrase ...“threshold to require reporting of attempts to compromise”. This led to discussion on intent, and how to determine the intent of the incident. L. Good suggested the group incorporate “an action which circumvents, disables, or renders ineffective, one or more of the security controls required for protection of BES assets, or associated PACS, EACMS, or PCA, regardless of practical impact to operation of the BES” into the definitions to clarify “Attempt to Compromise”. FERC staff, speaking for themselves, stated that it was important that the current definition of a reportable incident

retain the language “A BES Cyber System that performs one or more reliability tasks of a functional entity” when looking at applicability.

Project updates – next steps

T. Hall suggested the group conduct a review of the draft during the next teleconference, focusing on what makes an incident reportable. From there, Technical Rationale could be drafted with the goal of posting informally during the summer.

Action Item

- Drafting team to review R1 – R4 of current draft, considering how to revise language regarding what makes an incident reportable.

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 | 5/27/25 |
|------------------|------------------------------------|---------|
| Tony Hall | LG&E and KU Energy | Y |
| Sharon Koller | American Transmission Company, LLC | N |
| 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 |