NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

October 28, 2024 | 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 agenda for the call – the Drafting Team would focus first on the revised definitions, and then discuss concerns raised by M. Buchanan, who drafted the original SAR.

Revisions to Definitions

The group reviewed the definition revisions from the previous call, wordsmithing the terms to improve clarity.

> **Event of Interest** - Anomalous or suspicious conditions or activity that may indicate a cyber security impact, prompting the need for investigation.
>
> **Attempted Cyber Security Incident** -- An Event of Interest that, absent mitigations, indicates a potential cyber security impact, prompting the need for response.
>
> **Cyber Security Incident** -- An Event of Interest that indicates a cyber security impact, prompting the need for response.

Revisions to draft language

M. Buchanan shared concerns (included as Attachment 2) that the revisions to the standard were not clear enough in what activities should be shared with CISA. He shared a link from CISA to offer guidance, as well as a list of example activities that could be reported.

The group discussed the possibility of reviewing other CIP standards, and whether modifying them could help clarify the reporting processes in CIP-008.

Action Items

- Team should look back at CIP-003, CIP-005, CIP-006, CIP-007, CIP-010, (CIP-012? and CIP-013?) requirements that might hook into CIP-008, focusing on potential opportunities to modify the controls side of the equation to remove applicability/reportability decision from CIP-008.

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	10/28/24
Tony Hall	LG&E and KU Energy	Y
Sharon Koller	American Transmission Company, LLC	Y
Marc Child	Great River Energy	Y
Bryan Yoch	Ameren	Y
Joshua Rowe	WECC	N
Brent Howell	Duke Energy	N
Scott Klauminzer	Tacoma Public Utilities	Y
Lawrence Good	Bonneville Power Administration	Y

Attachment 2

From the SAR
Description-"provide a minimum expectation for thresholds defining an attempt to compromise."

DHS Cyber Security Reporting Initiative
https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

CISA's Sharing Cyber Event Information Fact Sheet contains a list of "activities that should be shared". This is not an exhaustive list but an example of how modifications to CIP-008 could be approached.

Example of CIP -008 R1 could be modified include criteria to evaluate and define attempts to compromise…

1.2 One or more processes:

1.2.1 That include criteria to evaluate and define attempts to compromise, which shall include, as a minimum, each of the following types of incidents:

1. Unauthorized access to your system
2. The presence of malicious code on applicable systems
3. Compromise of privileged accounts (Exfiltration of account information)
4. DDos attack on perimeter zones of trust outside the ESP that last more than 12 hours

Note: These are just examples. It can be debated whether these already meet the reportable definition or fall outside the CIP scope, but the point has more to do with the approach and not the specific examples that make the final cut.