NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

May 20, 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

Tony Hall, chair, began with an update on the current draft. He explained that he and Sharon Koller, vice chair, had discussions with FERC and NERC staff and some concerns were raised about the definitions in their current form. Overall, there was agreement with the direction the group had taken, but there were concerns that the definitions needed revision to ensure that the intent of the SAR was being met. Tony Hall requested that the drafting team consider this idea and that it would be one of the topics the group discussed during the planned revisions after outreach was conducted in July.

Outreach

First, the group reviewed the entities that had been identified for outreach, the DT member assigned to those entities, and if determined, the dates selected for presentation:

1. EEI - Tony Hall (*Week of 6/20*)
2. MRO NSRF – Sharon Koller (*6/26/24, 9-10 CDT*)
3. NPCC – Scott Klauminzer / Tony Hall (*6/25/24, 11 EDT*)
4. WECC WICF – Scott Klauminzer / Josh Rowe (*July*)
5. NATF/NAGF – Marc Child (*6/20/24*)
6. ISO/RTO/SRC – Alison Oswald (*6/24/24, 11:30-12:30 EDT*)

The team spent the remainder of the teleconference fleshing out the PowerPoint presentation based on the outline drafted during the previous teleconference (Attachment 2). The group agreed to utilize a format of listing the core changes for each requirement, then going into further detail, including a side-by-side comparison of the proposed language with the current language.

Attachment 1

Name	Entity	5/20/24
Tony Hall	LG&E and KU Energy	X
Sharon Koller	American Transmission Company, LLC	X
Darrel A. Grumman	Electric Power Engineers	N
Marc Child	Great River Energy	X
Bryan Yoch	Ameren	X
Joshua Rowe	WECC	X
Brent Howell	Duke Energy	N
Scott Klauminzer	Tacoma Public Utilities	X
Lawrence Good	Bonneville Power Administration	N

Attachment 2

- Project overview - Tony
  - Security objective
  - SAR
    - Results of NERC effectiveness study and FERC CIP audits / lessons learned
  - Priority / Timeline
- SDT approach - Sharon
  - Follow related INSM project
    - CIP-015
  - Consideration of other existing standards
    - CIP-004 – Events detected / Access reviews
    - CIP-005-6 R1.5 – Detect known or suspected malicious communications.
    - CIP-007-6 R3.2 – Mitigate the threat of detected malicious code.
    - CIP-007-6 R4.1 – Review log events.
    - CIP-007-6 R4.2 – Generate Alerts.
    - CIP-007-6 R4.4 – Review sampled logs to identify undetected Cyber Security Incidents.
    - CIP-007-6 R5.7 – Generate Alerts.
    - CIP-010-3 R2.1 – Deviations from existing baseline.
  - Brief update on formatting
- Overview of Revisions
  - Definitions – Scott K.
    - Starting with NIST definitions (realignment)
    - Removal of “requirement” language from definitions
    - Removal of scoping language from definitions
    - Retire Reportable Cyber Security Incident

- Conforming changes to CIP-003

- Core content changes in R1 – Larry G.
  - Shift from specific plan to cyber security plans
    - Sub bullets work collectively and in no particular order
    - Lean on existing plans that may be how EoI are detected
    - Provides clarity that Attempted Cyber Security Incident falls under scope
- Core content changes in R2 – Marc C.
  - Impact of shift to cyber security plans
    - Reversing 2.1 and 2.2
    - Conforming change to scope 2.2 testing to current enforceable
- Core Content changes in R3 – Josh R.
  - Incorporate use of identified deviations from R2 into 3.1
- Core Content changes in R4 – Josh R.
  - No changes to 4.1.
  - Changes to 4.2 – added Reportable Cyber Security definition added
  - No changes to 4.3
- Formatting changes
  - Remove tables in favor of structured outline
  - Simplification of Measures
- Visualization of process?
- Implementation
  - Looking at 12 month plan
    - Need to determine specifics for periodic requirements