NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

November 13, 2023

Review NERC Antitrust Compliance Guidelines and Public Announcement

Alison Oswald, 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.

Timeline Updates

Alison Oswald provided the drafting team with an update on the new NERC prioritization. NERC's strategy going forward is that only high priority projects will be posted for formal comment and ballot in the first half of 2024. This project is classified as medium priority so the team will only be posting for informal comment in 2024. The team will set up a meeting cadence of two meetings a month starting in January to continue to move froward with creating a draft post for informal industry comment.

Definitions Discussion

The team discussed rewriting definitions based on what constitutes a "Cybersecurity Incident" and what makes one reportable. The team also discussed standardizing vent vs incident in the standard language. A proposal for new definitions was presented by a team member.

a. *Cyber Security Incident*
   - *One or more malicious acts or suspicious events that*
     a. *accessed, collected, disrupted, denied, degraded, destroyed, or otherwise impacted the integrity, availability, or confidentiality of a system or its resources (Compromised system),*
     b. *attempts to gain unauthorized access to system services, resources, or information (Potential compromise through system access without observable impact), or*
     c. *an attempt to compromise system integrity, availability, or confidentiality (Potential compromise without accessing the system)*

b. *Reportable Cyber Security Incident*

- *Any of the above criteria which has occurred within or against a high or medium impact BES Cyber System, (1) an Electronic Security Perimeter (ESP), (2) a Physical Security Perimeter (PSP), or (3) an Electronic Access Control or Monitoring System (EACMS), or any other related events that disrupts or attempts to disrupt the operation of a BES Cyber System.*

The team discussed and considering adding PACS to applicable systems.

Finally, the team discussed the applicability of intelligence and the volume of sharing to the industry. Concerns were raised that the volume and collision of reports could lead to diminishing returns.

Attachment 1

Name	Entity	11/13
Tony Hall	LG&E and KU Energy	X
Sharon Koller	American Transmission Company, LLC	X
Darrel A. Grumman	Electric Power Engineers	X
Marc Child	Great River Energy	N
Bryan Yoch	Ameren	X
Joshua Rowe	WECC	X
Brent Howell	Duke Energy	N
Michelle Ross	Exelon	X
Scott Klauminzer	Tacoma Public Utilities	X
Lawrence Good	Bonneville Power Administration	X