NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

March 20 and 27, 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 on both days. The member attendance sheet is attached as attachment 1.

SAR Background

Michaelson Buchannan, NERC Compliance, provided an overview of the SAR to the drafting team (DT). A study was conducted in 2021 to improve visibility into report, but the counts have not changed from the 2018 standard drafting project. The compliance staff was expecting to see more reports. In general, the study found that entities were only looking if events pierced the ESP and not at attempts. Michaelson stated the team will have to find the right balance, as industry and NERC do not want a CIP-008 report on everything. Darrell Grumman asked if the team should be looking at IT and OT or BES Cyber Systems, to which Michaelson responded it would be up to the drafting team. Sharon Koller stated that the first team struggled with this definition and stated that if an entities' system is configured correctly, things will not arise to the level of attempts to compromise. She asked if those doing the study considered that the lack of report could mean that the industry is more secure than people realize, instead of the alternative that entities were given too much discretion to defining attempts for themselves. She stated that perhaps compliance staff did not like the discretion the SME's took in defining attempts for the organization. She continued to state that we do not want to distract industry or regulators with an abundance of reporting. Josh Rowe from WECC stated that he has looked at entities and believes that there are some gaps or applicability loopholes that could be tightened. CIP-005, 7, and 10 do not have ties back to incident response; only CIP-006 contains that, but only for physical breaches. It was suggested that the team focus on minimum expectations. Sharon Koller asked if there are other established frameworks that the team can look at for this. Michaelson suggested the kill chain and attack frameworks.

Team Introductions

Team introductions were conducted.

Revise SAR

The team reviewed the SAR form and discussed if standards other than CIP-008 should be opened. Josh Rowe stated comments from industry mentioned possibly providing more linkages with CIP-007, CIP-003, and CIP-001.

The team discussed what data there is to support that more reports were expected. Tony Hall stated that the previous team did not expect the revisions to trigger more reports. Additionally, based on how the changes were made, there is also a concern from industry that the previous version was not given enough time to be in effect. Maggie Steiner, FERC, stated there is a lot of good will that this project was stood up by NERC and not initiated by FERC order.

Darrell Grumman brought up his question from the previous meeting asking if corporate IT networks should be included or not for this project. Currently only PACS and EACMS are in scope. Marisa Hecht, NERC Legal, stated corporate networks should not be included.

Josh Rowe stated the EISAC report from September 2019 might be helpful for the drafting team in terms of helping us to understand what EISAC really wants to know.

The team modified the detailed description of the SAR to move some language into the drafting phase of the project.

Attachment 1

Name	Entity	3/20	3/27
Tony Hall	LG&E and KU Energy	X	X
Sharon Koller	American Transmission Company, LLC	X	N
Darrel A. Grumman	Electric Power Engineers	X	X
Marc Child	Great River Energy	N	X
Bryan Yoch	Ameren	X	X
Joshua Rowe	WECC	X	X
Brent Howell	Duke Energy	X	X
Michelle Ross	Exelon	X	X
Scott Klauminzer	Tacoma Public Utilities	N	X
Lawrence Good	Bonneville Power Administration	X	N