NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

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

October 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. quorum not met initially by attendance, but the decision to continue the conversation was made as we were expecting quorum halfway through. The member attendance sheet is attached as attachment 1.

Opening Remarks
Sharon Koller recapped the team's previous meeting and work thus far. It was mentioned that the INSM work proposed by FERC might merge into the CIP-008 standard.

Review Definition Notes
The team began by discussing the definitions. Proposed adding to the current definition to expand what should be reported without necessarily defining "attempt to compromise".

The team had a concern that the use of "Disruption" in the current language might allow non-reporting in the current language of the standard. The team discussed potentially moving back from "disruption" to alerts/events from the systems to (potentially) "compromised" devices that don't lead to a disruption in the system.

A fourth bullet was added to the desired output from the reportable criteria to include the "disruption" severity in the potential compromise analysis chain. The team felt it might be beneficial to reverse the order so that the standard does not need to be completely redone, but can instead add the additional information desired by NERC/E-ISAC to the current standard.

A concern was raised that the current standard defines the requested output from the ESP/EACMS, but this might not be adequate as the detection of the "attempt to compromise" might come from systems outside of these roles/environments.

Standard Revisions Discussion
The team discussed a question related to expanding the scope of covered system to PCAs/PACs.

It was suggested to add "detecting" to the required event criteria along with "containing and eradicating". The team worked on crafting new language to tie the standards together to define order of operations for investigating which include the criteria for reporting. The team discussed starting from a blank page to start fresh to redefine the standard.

Started discussions around requirement R1 and the order of operations. Additionally, the team discussed what constitutes a "security event" vs an "incident" and when the former becomes the latter.

Attachment 1

Name	Entity	10/13
Tony Hall	LG&E and KU Energy	N
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	X
Michelle Ross	Exelon	X
Scott Klauminzer	Tacoma Public Utilities	N
Lawrence Good	Bonneville Power Administration	X