NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

April 27, 2023 | 3:00 – 4:30 p.m. Eastern

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.

Team Research Discussion

Josh Rowe from WECC presented redacted audit findings including AOCs and recommendations related to attempts to compromise. Entities did not identity thresholds was a common theme. Also, he presented that no comprehensive definition of attempts to compromise was found.

Tony Hall gave an example of a threshold in his company of three-to-five bad password attempts being a trigger, but would require more investigation before it's reportable. Tony asked Josh if the underlying thought is that there need to be more guardrails around allowing professional judgement. Bryan Yoch stated that the problem with setting thresholds is that the adversary would need internal foothold first, and if they did, they would try low and slow to remain undetectable. Marc Child stated he believes attempt to compromise is a problematic issue, as it implies that the defender knows the intent of the adversary. Joseph Gatten suggested the team think of thresholds that can be used to trigger an investigation, but not be used as a criteria for reporting. Barry Kuehnle from FERC stated the language "where entity makes a determination" in the existing standard is what allows the entity the latitude to have a strong definition or not. Josh gave an example of scanning a device or coming across a log entry that requires some response should be considered "events of interest" and trigger the investigation. He agrees that malicious intent is a problematic notion. Joseph stated blocking a known virus is a simple example of an everyday event that might be an incident, but should never trigger an investigation or hit a threshold. Bryan reminded the team that these assets are protected in internal zones and that the relative threat is much lower than in the corporate/internet zones. He asked if the team should align requirements to the tools used to support CIP standards such as CIP-005, CIP-006, CIP-007, and CIP-010. Tony thinks we must maintain latitude in requirements due to entities individual architectures. Michelle Ross expressed a concern about opening things up too broadly and the opposite problem happens; there are too many incidents and reports.

Barry stated there is a point during any investigation where a decision can be made whether it should continue (or not) after finding something suspicious. As an example, spear-phish to a person with a highly relevant or novel malicious link and was caught, which would normally trigger an everyday share with E-ISAC. He asked how many people would consider that an attempt to compromise. In response, a few SDT members responded with yes. In defense of Yes, some team members stated that the idea is to get this information to entities who may not have the capability to detect/block the same attack. In defense of No, other team members stated there is a corporate-environment attack and can't be traced to a CIP attack vector. Tony stated another example, a TCA that gets caught in the example Barry provided, gets infected, and then connects to a CIP asset. Larry stated he does not think using email is a productive example for purposes of CIP-008. He also stated we should not forget there are other areas such as CIP-013, where incidents can exist and require handling by the entity. He asked if malware detected in vendor software should be a CIP-013 issue and fall out of scope of CIP-008. Tony stated in the previous project the EISAC briefed the group that they really don't much care how incidents are reported to them. Sharon Koller agreed with Tony that using a form allows the entity the better document for compliance purposes. Bryan asked if the industry is already overwhelming the E-ISAC with volunteered IOCs. Sharon stated that good mature programs should triage common explainable things, and only report that which is novel or actionable. Barry agrees that the team needs to focus on applicable systems. Joseph stated for auditability, the team should focus on the investigation process and the artifacts generated. Tony describes his company's process of having a generic corporate response plan that handles all incidents the same way regardless of the regulatory requirement and he thinks it sounds like others have similar situations. Tony ended the meeting by stating this was a good discussion today that sets a baseline of understanding what we can build on for future drafting.

Attachment 1

Name	Entity	4/27
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	X
Michelle Ross	Exelon	X
Scott Klauminzer	Tacoma Public Utilities	N
Lawrence Good	Bonneville Power Administration	X