NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

August 7 and 11, 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.

CIP-008 Standard Revisions

August 7, 2023

The team reviewed the current NERC definitions of Cyber Security Incident and Reportable Cyber Security Incident. The current definition of a CSI includes Compromise, Attempts to Compromise, Disrupt, and Attempts to disrupt. The team asked how can this standard drafting team clarify these terms? Team members also noted that "intent" is a factor in suspicious or malicious activity and the team needs to consider this in discussions. The team discussed the differences between compromise and disruption. Team members stated that entities can have a Cyber Asset that is compromised without disrupting the operation of a BES Cyber System. A team member asked if the team should replace "suspicious" with "anomaly"? It does not say something is malicious, it just says something needs to be investigated. Something out of the ordinary occurred and it needs to be investigated to determine the cause. The team wants to remember that the intelligence gained from a Cyber Security Incident needs to be actionable and useful.

Defined Term Revision

The following are the team's initial draft thoughts on possible revisions to defined terms.

<u>Cyber Security Incident</u>

- CSI - events generated by (in scope) monitoring systems that require investigation. (Triggers)
- An event that requires activation of the Cyber Security Incident Response Plan.

<u>Events of Interest</u>

- Anomalous activity at an Electronic Security Perimeter, Physical Security Perimeter, or an EACMS. Triggers an investigation or assessment to determine if the anomalous activity requires triage or response actions.

Reportable Cyber Security Incident

- Artifacts from an investigation that are actionable and can be consumed by other utilities to strengthen their own defenses.

August 11, 2023

The team began discussing potential areas to revisit the standard language. R1.2.1 around attempt to compromise was the fundamental candidate for modification and there was a recommendation around building the criteria around attempt to compromise with section 1.3 being the first stage (Identify-Triage-Classify). The team discussed the possible paths of standard language modification listed below.

Suggestions around modification language:
R1: Create a plan
R2: Implement test plan
R3: Updating when change
R4: reporting timeframe

Additional suggestions around modification language:
R1.1: Incident Response Process
R1.3 and 4: Subset of what is included in the process

Additional suggestions around modification language:
R1.1: Incident Response Process
R1.2: Roles and Responsibilities
R1.3: Incident Identification/Event of Interest – Physical or Cyber
R1.4: Incident Classification (CSI, RCSI, Attempts, Benign)
R1.5: Incident Handling/response procedures

Additional suggestions around modification language:
Proposed NIST CSF v 2.0

1. The plan is executed
2. Analysis happens

2a. Forensics artifacts held

3. Internal and external notifications happen

3a. Voluntary information sharing occurs

4. Contain and eradication

The team discussed an overall issue is the lack of incidents reported, specifically around the attempt to compromise. Members stated just because one entity stopped the incident does not mean others will too, so it is helpful to get that information out in the "community". There were some concerns among the group around potentially people may be unclear in what is meant in "classify" and perhaps there is an opportunity to come up with a matrix to help alleviate this ambiguousness.

Attachment 1

Name	Entity	8/7	8/11
Tony Hall	LG&E and KU Energy	X	X
Sharon Koller	American Transmission Company, LLC	X	X
Darrel A. Grumman	Electric Power Engineers	X	N
Marc Child	Great River Energy	X	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	X	N
Lawrence Good	Bonneville Power Administration	X	N