NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

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

August 21 and 30, 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.

Continue CIP-008 Standard Revisions
August 21, 2023

Tony Hall had opening remarks to the team that we will be working on drafting language of the requirements and potentially definitions. Sharon Koller states that definitions may be problematic, but the order of operations within the requirement may make it difficult to modify the definitions. Tony asked the team which area they would like to discuss first and the team decided on definitions.

The team began with the currently approved definitions on screen and began to modify. T. Hall stated we should be careful with definitions due to Cyber Security Incident being referenced in CIP-003. Darrel Grumman stated that order of operations should apply to universal impact before more specific impact, such as all BES then high and medium. Josh Rowe noted that timeliness of reporting to E-ISAC may be modified too. Scott Klauminzer supported the order of operations change to put disruption above attempts to compromise. T. Hall asked if the wording should be the same for compromise and attempts to compromise. S. Koller stated the disrupted component is in both definitions. Disruption is both an incident and a reportable incident. Compromise is only in the attempt definition. The team asked if a cyber security incident is only a real compromise or is it an incident worthy of investigation to determine if it is a compromise? Common mindset of the team is that a compromise is an actual compromise.

T. Hall stated we need to be aware people may be shifting the definition to be most favorable depending on their circumstances. Observer Shawn Null stated an attempt to compromise is having a foot on it, not necessarily a change to or disruption of the system.

T. Hall states the term is used in CIP-003 to determine when reportable and who to notify. S. Klauminzer asked for clarity on listing BES Cyber Systems, they may exist at lows and CIP-003 requirements may apply, even though CIP-002 doesn't require listing lows by individual BES Cyber Asset. T. Hall stated CIP-003 can be applied at facility level for lows or can list them and apply them more granularly.

S. Klauminzer suggested an order of operations: anomaly, attempt, and incident. Anomaly is a possible indicator of an incident; an incident is a successful attempt. Suggestion to take out attempt because a suspicious event leads to a potential incident. Whether something becomes an incident depends on how far it gets before blocked.

S. Koller expressed concern that we are compounding the issue by keeping attempts to disrupt and attempts to compromise when an attempt to compromise is also an attempt to disrupt. Marc Child believes streamlining disrupt and compromise makes more sense, not keeping both. Another suggestion was attempt defined as "*to gain unauthorized access or use the system in an unauthorized manner*."

Suggestion from an observer with Ameren for attempt as, *"An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity."* Another possible extended definition could be, "*The intentional act of attempting to bypass one or more security services or controls of an information system."*

T. Hall asked if there are definitions in use by other federal agencies that we could use, such as NCICC or CISA. He stated that the Cybersecurity Incident process cannot be started until something is detected, except if notified by outside agencies of industry activity. Observer Barbara Weber supports tying into federal level definition from CISA/NIST. For most entities, cybersecurity incident response processes/programs/response is at corporate level, not specific to only BES CSI. Need a program that can respond to all federal regs. So, a unique definition for NERC CIP is undesirable. T. Hall did some research and stated multiple "federal definitions" exist. J. Rowe stated regional interpretations may be difficult.

T. Hall suggested moving to second part "reportable" cyber incident. S. Koller asked if we have solved ambiguity around "attempt"? Does attempt require an identifiable bad actor? S. Klauminzer stated the benefit of reporting is information sharing with others.

T. Hall informed the team the next meeting was Wednesday, August 30. The team will start with drafting requirement language, keeping draft definitions in mind from today. The team did not finalize definitions today, pending some possible adjustment to the definition language.

Life Cycle of an Event

August 30, 2023

The team discussed the life cycle of an event to focus the revisions to the standard or definitions later on during the drafting phase. Created a list of actions/steps that would occur during an incident response:

1. Entity becomes aware of some event (could become aware through multiple different channels)
2. Ticket generated that goes to an initial response group
3. Initial analysis of the event

   a. Impact analysis to determine if it was:
      i. Nothing (process stops)
         1. Entity asks is it a test, false positive, non-NERC environment
      ii. An attempt to compromise
         1. Output of security controls put in place for CIP-003, CIP-005, CIP-006, CIP-007, and CIP-010 (for baseline monitoring)
         2. ICS targeting; or
         3. An inexplicable or anomalous event (or series of events) that the Responsible Entity has determined through investigation was an effort to cause a Cyber Security Incident
      iii. Actual compromise
         1. Anything that circumvents CIP-003, -5, -7, and -10
         2. CIP-006 (conditional)
   b. Applicable systems/environments check

4. Impact analysis determines either attempt or compromise

The team was instructed to review notes and definitions drafted and bring additional ideas and thoughts to next meeting to continue work.

Attachment 1

Name	Entity	8/21	8/30
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	N
Brent Howell	Duke Energy	N	X
Michelle Ross	Exelon	X	N
Scott Klauminzer	Tacoma Public Utilities	X	N
Lawrence Good	Bonneville Power Administration	X	X

NERC Antitrust Guidelines

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Public Announcement

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

NERC Standards Development Process-Participant Conduct Policy

http://www.nerc.com/pa/Stand/Documents/Standards%20Development%20Process-Participant%20Conduct%20Policy.pdf

NERC Email Listserv Policy

http://www.nerc.com/pa/Stand/Documents/Email%20Listserv%20Policy%2004012013.pdf