NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

April 28, 2025 | 2:00 – 4:00 p.m. Eastern

Review NERC Antitrust Compliance Guidelines and Public Announcement

Jason Snider, 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.

Opening Remarks

T. Hall, chair, welcomed the group and gave an overview of the goals for the call – determining which approach the group wanted to proceed with (an EOP-004 style table or adding language to the measures), and then discussing how to prepare for an informal posting.

Project updates - posting

T. Hall informed the drafting team that low-priority projects were able to post informally, and suggested the group work towards posting in the near future to gather feedback and avoid rehashing topics. The drafting team discussed how an informal posting would provide the opportunity to collect comments on the language, and that though not required, effort would be made to respond to comments received.

Project updates – next steps

The group held an informal (due to not reaching quorum yet) poll on which path the group should pursue – an EOP-004 style table or focusing on adding language to the Measurements. All five drafting team members present chose focusing on Measurement language. There was discussion around whether or not the group would need to revert to a table for Measurements. T. Hall noted that the intent was not to be too prescriptive. This led to discussion on the Technical Rationale document, and whether examples would be better suited to be included in the Measures, a Technical Rationale document, or as an attachment.
The drafting team reviewed the current draft of R1:

R1. Each Responsible Entity shall document one or more cyber security plan(s), for high and medium impact BCS and their associated EACMS and PCAs, that collectively include processes to: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

1.1. Analyze and classify Events of Interest.

1.2. Respond to Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident;

1.3. Identify the roles and responsibilities of response groups or individuals;

1.4. Manage incident handling procedures for Cyber Security Incidents; and

1.5. Notify applicable agencies pursuant to Requirement R4.

S. Koller suggested the group consider incorporating language similar to what was added to CIP-010-5 to R1.1:

1.1. Analyze and classify Events of Interest , *which at a minimum include events, alerts, or alarms detected by one or more requirement parts in CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, or CIP-015*.

This was well received by the group. M. Child suggested the group consider taking this approach further and add the language to the current standard, forgoing the previous changes the group had worked on. The drafting team agreed this could address the SAR with minimal impact, though it was noted that some clarity may be needed to avoid requiring everyday occurrences, such as a successful login to be flagged as Events of Interest.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; which at a minimum include events, alerts, or alarms detected by one or more requirement parts in CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, or CIP-015. 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	

T. Hall suggested the next steps for the language would be to review with staff from NERC and E-ISAC for feedback.

Action Items

- Drafting team to consider proposed language change and be prepared to discuss further on next teleconference.
- J. Snider to set up meetings with drafting team chairs and NERC staff to discuss proposed language.

Parking lot

- Definitions
- Feedback on use of “may” in definitions
- Definitions – what is being impacted?
- Coordination with DOE 417 (updating external forms)
- Applicable systems
- Include specific language in each primary requirement
- Requirement language
- Technical Rationale
- Implementation Guidance
- Updating slide deck

Attachment 1

Name	Entity	4/28/25
Tony Hall	LG&E and KU Energy	Y
Sharon Koller	American Transmission Company, LLC	Y
Marc Child	Great River Energy	Y
Bryan Yoch	Ameren	Y
Joshua Rowe	WECC	N
Brent Howell	Duke Energy	Y
Scott Klauminzer	Tacoma Public Utilities	N
Lawrence Good	Bonneville Power Administration	Y