NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2018-08 CIP-008 Modifications to Cyber Security Incident Reporting Standard Drafting Team

December 4, 2018

Conference Call with Web Access

Administrative

1. **Review NERC Antitrust Compliance Guidelines and Public Announcement**
2. **Roll Call and Determination of Quorum**
   The rule for NERC Standard Drafting Team (SDT or team) states that a quorum requires two-thirds of the voting members of the SDT to be physically present. Quorum was achieved as 10 of the 12 members were present.

Agenda Items

1. **Chair Remarks**
   The chair congratulated the team on a successful second ballot. Chair also notified the team that the team will be presenting to the CIPC during our in-person meeting
2. **Review steps for Final Ballot**
   Reviewed documents that will be needed for final ballot including a summary of comments report to address the comments received on the second ballot.
3. **Present suggested clarifying changes to standard**
   Two potential non-substantive changes were presented to the drafting team for consideration.

   a. Cyber Security Incident Definition – As written, the revised definition only makes the association to EACMs for High and Medium BES Cyber Systems think of this as the disqualifier for lows. However entities could most definitely will have an ESP and PSP by definition at lows even though there are currently no applicable requirements for those “things” that meet the definition. Therefore a compromise or an attempt to compromise the firewall (meets the definition of an EACM) at a low would not be reportable but if the compromise also was targeted to that “thing” that meets the definition of an ESP or PSP it would be reportable. To be more precise, the suggestion is that, the association (disqualifier for lows) needs to apply to all 3 listed definitions to exclude lows. This could be done by putting the high and medium systems in the beginning such as:

      Cyber Security Incident:
      A malicious act or suspicious event that:

- For High and Medium BES Cyber Systems, compromises, or was an attempt to compromise the, (1) Electronic Security Perimeter, (2) Physical Security Perimeter, or (3) Electronic Access Control and Monitoring Systems; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

b. Requirement 1.2.1 – Where the standard states "One or more processes to" "1.2.1 Establish criteria…." is not working. The concern is that as worded entities would be required to have a process to establish criteria, but not actually have criteria to evaluate and define attempts to compromise. Suggested possible clarifying changes are "One or more processes that include", and "Criteria to evaluate and define attempts to compromise" which seem to better describe the teams intentions.

4. **Present clarifications to supporting documentation**
Some clarifying changes to each document have already been identified and were presented to the team as work that will need to be done during the in-person meeting.

a. Technical Rationale – There are a few mentions of "reportable attempted cyber security incident" that remain in the document that need to be removed. In addition there are a few areas in the technical rational where the language does not match the standard or what is in the Implementation Guidance. One of these that will need to be modified is the areas that discusses the "methods for submitting" the attributes required in the standard. Finally, there were some diagrams that were copied from the GTB in the standard and put into the Tech Rationale that were cut off and need to be recopied.

b. Implementation Guidance:

i. P10- Intermediate remote access was identified as IRA when that term is used to refer to Interactive Remote Access which is a NERC defined term.

ii. P13 – Example N4 needs clarification

iii. P19 – the color used in the chart corresponded to the same colors from the classification scheme on P11 but the team needs to confirm that the colors match the scheme appropriately.

iv. P20 – example that included malware, suggestion to remove the word "enterprise" in front of windows

5. **Comments discussion and assignments – D. Rosenthal and K. Martz**

a. **Proposed modifications to definitions – Cyber Security Incident and Reportable Cyber Security Incident (Q1)**
The SDT received a large amount of comments on this question. Many commenters still requested the SDT to define "attempt to compromise". Included in the comments were a few suggestions on updates to the definitions. The comments were split about evenly on if PCA's should be in or out of scope.

b. **Definition of attempts in defined criteria – (Q2)**
The SDT received a large amount of comments on this questions. Again, comments were received that asked for "attempt to compromise" to be defined. A comment was received that the language that ties R1.2 to R4 could cause a double jeopardy situation for entities.

c. **Process to determine "attempt to compromise" and provide notification (Q3)**
The SDT received a large amount of comments on this question. A few commenters stated that R4.2 stands on its own and that R1.2 is not needed. More comments received that allowing entities to define attempts for themselves might make reporting inconsistent. A few commenters also suggested the removal of the word "only" in R1.2.2.

d. **EACMS in Scope (Q4)**
Majority of responses to this questions were positive. One commenter remarked that EACMS that only perform monitoring functions should not be in-scope because of the low risk. A separate comment stated that the way the SDT addressed EACMS could be confusing and bring low impact devices into scope. An additional commenter stated that considerations related to Project 2016-02 that should be considered in the scoping of CIP-008.

e. **Reporting Timeframe (Q5)**
Majority of responses to this question were positive and agreed with the SDTs proposed reporting timeframes. A few entities requested additional clarifying language related to attempts that turn in to incidents. One comment received requested coordination in reporting through one agency and if that was not possible requested 2 hours for initial notification instead of just 1 hour. A few commenters expressed concerns about the administrative burden of the updates and there was a final request to align CIP-008 reporting timelines with OE417 and EOP-004.

f. **Notification Method (Q6)**
Majority of responses to this question were positive and agreed with the SDT's decision to give the responsible entity the flexibility to determine notification methods. There were a few comments that requested a consistent reporting for or for alignment with the EOP-004 and OE-417 reporting forms. In addition there were a minority of responses that did not like the removal of R4.2, which listed three different methods for providing notification, because the opinion was that the inclusion was comprehensive.

g. **Implementation Plan (Q7)**
Majority of responses agreed with the SDT's decisions to increase the Implementation plan time frame from 12 to 18 months. A minority of responses stated that they still want 24 months because of the burden the changes will have on smaller entities. Only one response was still in support of the original 12 month plan.

h. **VRF/VSLs (Q8)**
Majority of responses agreed with the proposed VRF and VSLs for the draft standard. A few responses pointed out that for R4, there seems to be duplication of criteria for Severe and High VSL regarding the following: "The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4)", which shows up in both columns

(Severe and High VSL). There were an additional few comments about some of the administrative aspects of the standard being too high on the VSL rating. A final few comments did not agree with the VRF/VSL's because of underlying problems with the standard language.

i. **Cost Effectiveness (Q9)**
Multiple comments received stated that double reporting is not cost effective and requested coordination through one agency, i.e. E-ISAC is responsible for reporting to NCICC. One comment stated that the timelines for reporting may create additional burden and cost for entities. Another response stated that this entity would have to set up a security operations center which would be extremely costs.

j. **Other comments (Q10)**
The SDT received many responses to this question, some of which were received in previous questions. One commenter responded that in R2.2 language is added that states: "…that attempted to compromise a system identified in the "Applicable Systems" column for the Part,…". It is not clear to which Requirement Part the "Applicable Systems" column for the Part" is referring to. Xcel Energy recommends adding the part number (i.e. Part 2.2) to each occasion where a Requirement Part is referenced with the Requirement Language or removing the references to the Part altogether. Another comment on R2.1 stated it should be modified permit exercise of the plan using any Cyber Security Incident. Restricting the exercise to only Reportable Cyber Security Incidents restricts the exercise to only a subset of an entity's incident response plan. One comment was received that wants CEC language in standard. A handful of comments included suggested modifications to Implementation Guidance.

6. **Objectives for in-person meeting**
The objectives for the next in-person meeting are the clean up the standard, Technical Rational and Implementation Guidance Documents to prepare for final ballot.

7. **Review Project Timeline**
The next team meeting will be held December 11-13, 2018 in Atlanta, GA at The Whitley Hotel. We will start the meeting on Tuesday at 830 am Eastern. Final ballot will be conducted in January 2019

8. **Adjourn**
The meeting adjourned around 3:20 p.m., Eastern, December 4, 2019.

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