NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

October 29, 2018

Conference Call with Web Access

Administrative

1. **Review NERC Antitrust Compliance Guidelines and Public Announcement**
2. **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. Quorum was achieved as 11 of the 12 members were present.

Agenda

1. **Chair/Vice Chair Remarks – D. Rosenthal**
   The work ahead of the SDT will focus on responses to comments. A quick Pareto analysis was preformed which ranked in order (highest to lowest by frequency) those items that drew the most controversy in the initial draft of the standard. The approach needs to be adjusted in seven key areas which are listed in Agenda Item two below.
   - This helps bring the BIG WINS to the top of the list which will provide the most positive impact when socialized with industry and government.
   - The SDT met with E-ISAC and ICS-CERT (now the NCCIC) to understand information sharing options. Through great collaboration, the SDT has developed a new strategy.
   - From an outreach/socialization perspective, the SDT is going to meet with groups to ensure that the SDT meets the mark. The team will engage stakeholders for assistance and support. The team heard the concerns expressed by the industry and is working on making the necessary changes.
   - In areas where the team needs to strike a balance, necessary actions will be taken to ensure industry's concerns are addressed.
2. **Review Top Areas – A. Oswald**
   The top concerns/issues from industry that were received from the comment period were reviewed as follows:

- **Attachment 1**
  Industry does not want to require the attachment, only the three attributes that need to be reported.
- **Notification Approach**
  - Some entities are asking for additional time for initial notification.
  - Confusion that initial notification and updates are not required until an incident is "determined" by an entity to be reportable or reportable attempted.
  - Industry does not want to submit to two agencies; multiple comments received regarding this.
- **Attempts**
  - Industry wants a definition.
  - Industry has concern over auditors not agreeing with the entities definition of "attempts".
- **PSPs**
  How do PSPs fit into CIP-008, if at all?
- **EACMS**
  Industry is concerned that the scope of EACMS is increased by calling out the five functions.
- **Implementation Plan**
  Industry thinks time should be longer 18-24 months; regions think it should be six months.
- **Cost Effectiveness**
  There are concerns on what "attempts" means and if it would require more personnel to deal with the reporting requirements.

3. **Discuss E-ISAC and NCCIC (ICS-CERT) review from Friday – A. Oswald**
   A conference call with representatives from E-ISAC and ICS-CERT was held with the team on Friday October 26, 2018. The team discussed the concerns from industry surrounding multiple issues. The SDT first asked if a form is required by either agency. It was learned that neither will require the three attributes to be submitted in a standardized form. However, DHS did state that the more standardized the information that comes in is, the easier it is for them to digest and less they will have to reach back out to the entities to gather information. Second, how industry can submit information to each agency was discussed. Both agencies accept phone calls, email, and secure website submissions. In regards to submitting confidential information, both indicated they have PGP available, and their website submissions have security as well. DHS also has an XML schema. Once the information is at E-ISAC it will be treated the same as it is for other security-related mandatory reporting. Both agencies indicated they will never attribute information back in an entity. There were comments about having one agency be the primary and forward the information on to the other agency but unfortunately that will not be possible. Neither agency can be responsible for the registered entities compliance with submitting to both agencies nor will they forward anything to the other.

4. Begin Standards Updates

The team began modifications to the draft CIP-008-6 with the attachment, the notification timeframes and the notification methods. These topics are covered in questions 3, 4 and 5 form the comment form. The individuals assigned to these questions are responsible for writing the response to comments that will be included in the summary report. There is a draft of this report saved on the share point site. After this discussion and no later than next Tuesday draft responses to these comments should be entered into that report. Also, as we go through this discussion, if there are unique comments from those questions that are not covered in this discussion, please bring them to the attention of the team and be prepared to include that question and answer in the comment report.

Attachment 1 and Notification Approach

1. Attachment 1 – The team made a choice to remove the attachment form the standard since neither agency, E-ISAC or ICS-CERT will require it. Attachment 2, instructions for completing Attachment 1, was also removed from the standard. These will both be placed into Implementation Guidance as an example of one was an entity could comply.
2. R4.1 – Measures modified to remove reference to Attachment 1. A team member pointed out that there is also an issue with the use of "reportable" in R4.1 requirement. This will be revisited during the upcoming discussion on PSPs.
3. R4.2 – The team removed this requirement completely because industry feedback did not like the prescriptive nature of listing three different methods in which they could contact E-ISAC or ICS-CERT. It was discussed to include a generic phrase such as "in an E-ISAC or ICS-CERT" approved method in R4.3 below which deals with time frames.
4. R4.3 – This is the new R4.2 for Draft 2 of the standard. After discussion, the team did not include the phrase discussed above and will remain silent on the "how", focusing on the "what". R4.3 simply requires entities to report to both agencies under two different timelines depending on what type of incident they have experienced.

   The team discussed the one hour reporting requirement for a Reportable Cyber Security Incident. The requirement was written to read that registered entities are required to notify both agencies within one hour. There are industry concerns that the time period is too short to notify two agencies. An example given was that if an entity was experiencing a Reportable Cyber Security Incident and called one of the two agencies to report and ask for assistance, that phone call could last over an hour and then they would not be compliant with this requirement when they were simply seeking assistance in dealing with an issue. Industry suggests that the time frame should be two hours. The team discussed this possibility. It was pointed out that FERC order 848 p89 say the timelines need to be risk-based. A representative from FERC (speaking only for himself and not on behalf of the commission) said a two hour timeline might be questionable. The team decided to table this discussion until a future meeting.

The SDT discussed "calendar day" in the reporting of a Reportable Attempted Cyber Security Incident. Industry suggests updating this to "business day" because there are concerns over having adequate staff over weekends, holidays, and after hours. It was discussed that this was after determination, so perhaps some of the industry concern was based on a misunderstanding of when the reporting time clock began. It was pointed out that FERC order 848 made mention of reporting timeframes for initial notification between 8 and 24 hours and the "next calendar day" was already on the long end of that range. "Next business day" could potentially be a four or five day gap if any holidays come in to play. The team decided to table this discussion until a future meeting.

5. R4.4 – This is the new R4.3 in Draft 2. Industry requested updates be reported within seven days instead of five. While some industry comments were based on a misunderstanding that updates are required every five days instead of the team's intention that once new information is determined, then the entity should report within five days, the team decided to change the time to seven days. This would align better with entities' operations that might have on-call schedules of seven days. It was mentioned that the team needs to promote their message of "determination" being the start of time clocks for reporting to industry.

   It was also discussed that this requirement language can be modified to make the teams intention clearer on when submissions should occur. Industry suggested some sort of final submission report. This was tabled for discussion at a future meeting.

5. Discuss "Attempts" (review approach) – A. Oswald

The team began a discussion about the industry feedback around the word "attempts". The comments were around two issues, either entities want a definition to support audit situations or the team needs to make it clearer that entities are to define this for themselves. While "attempt" was in the CSI definition before, it was never actionable and now that it is, industry wants to know what it means. The team discussed what defining the term "attempts" would mean. There were many comments raised that said no matter how it is defined, something is going to be forgotten, the list would be long, incomplete and by the time it is published probably out of date. The option of discussing attempts in IG was discussed. This could show an entity one way that could try to define "attempts" for themselves and map it back to other standards at a minimum such as the monitoring required in CIP-007 and CIP-010. It was pointed out that if we defined "attempts", there would also be a large group of entities that would have negative comments. Those that are comfortable defining it themselves have well developed CIP programs currently in place.

FERC Order 848 p55 gives some background on how FERC defined "attempts". The objective is to report suspicious activity that could benefit other entities.

Concerns that auditors will not agree with an entities definition of "attempts" was also discussed. NERC Compliance Assurance representatives stated they felt the standard as written was fine. It is the auditor's job to get an understanding of the entities process in place and conduct an audit to that. It was also stated that there are other requirements written in a similar fashion already enforceable today. Discussion on this subject will continue at a future meeting.

6. **Future meetings**
   a. November 1, 2018 – Conference call
   b. November 6-8, 2018 – Houston, TX
7. **Adjourn**
   The meeting adjourned at 4:30 p.m., Eastern, October 29, 2018.