NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2014-02 Standard Drafting Team

March 18, 2014 | 9:00 a.m. – 5:00 p.m. PT
March 19, 2014 | 8:00 a.m. – 5:00 p.m. PT
March 20, 2014 | 8:00 a.m. – 12:00 p.m. PT

Sacramento Municipal Utility District (SMUD)
6301 S Street
Sacramento, CA 95817

Tuesday, March 18

1. **Welcome**

   NERC Staff welcomed observers and participants to the second face-to-face Standard Drafting Team (SDT) meeting.

2. **Introductions and Safety Briefing**

   SDT members and observers introduced themselves and SMUD Staff gave the safety briefing.

3. **NERC Antitrust Guidelines and Public Meeting Notice**

   The NERC Antitrust Guidelines and Public Meeting Notice were read.

4. **Update on FERC Order on Physical Security**

   NERC Staff involved in Project 2014-04 Physical Security provided an update on development activities. FERC Staff left the meeting during this discussion to comply with ex parte communications rules.

5. **Determination of Quorum**

   The rule for a NERC Standard Drafting Team (SDT) states that a quorum requires two-thirds of the voting members of the SDT. Quorum was achieved as 9 out of 10 SDT members were either present or dialing in via ReadyTalk.

6. **SDT Progress Summary**

   The SDT co-chairs presented a summary of the SDT's activities the past two weeks. They provided details of each subgroup's approach during the previous weeks.

   NERC Staff and Standards Committee members attending the meeting discussed the new balloting software. Project 2014-02 will be in the new software, and entities will need to register to become a part of the Registered Ballot Body starting April 1. Project 2014-02's ballot pool will form during the first 30 days of the comment period. NERC Staff encouraged meeting participants to attend NERC's upcoming webinars on how to use the new system. The first webinar will be April 8.

7. **Reliability Assurance Initiative (RAI) Presentation**

   NERC Compliance and Enforcement staff presented a sample application of RAI to a CIP requirement for a hypothetical entity. The presentation slides are available here.

8. **Identify, Assess, and Correct (IAC)**

   Meeting participants discussed how the information from the RAI presentation impacts the SDT's approach to the IAC directive. The SDT discussed the option to insert self-correcting language in the standard but the SDT stated this would add two compliance obligations: the performance requirement and the IAC obligation. Entities could be in violation of both if the language is used. The RAI presentation helped level the knowledge among SDT members, although some confusion and concern remains over the implications of removing IAC. The SDT determined that it needed to develop a document to explain its rationale for removal of IAC language. The SDT developed the following action items for the IAC subgroup:

   - Develop Frequently Asked Questions or informative documents regarding relationship between 17 IAC requirements and RAI; keep focus on where RAI/IAC interact (present on 3.31.14 Full SDT call)
     - Document 3.18.14 presentation
     - Work with NERC Compliance/Enforcement to ensure document is consistent with approach and confirm common understanding
     - Gather questions and concerns from industry to answer in document or submit to compliance/enforcement (subgroup call 3.25.14)
     - Consider how this document will be distributed/life of language
   - Review 17 requirements for whether clarifications may be needed in language (e.g. timeframes?)

9. **Communication Networks (CN)**

   The SDT provided an overview of the work discussed on the conference calls.

   The SDT discussed the protection of nonprogrammable components in the CIP-006-5 proposed language. Meeting participants suggested that the subgroup consider what is in and out of nonprogrammable components. The SDT did not think a Glossary definition was necessary, but the SDT would consider developing guidance on what are considered nonprogrammable components.

   The subgroup had included a requirement to restrict physical access to nonprogrammable components, encrypt the data on these components, or to monitor and respond. The SDT discussed whether data encryption or monitoring the nonprogrammable components are appropriate alternatives to restricting physical access, noting the scope of Order No. 791. The SDT determined to keep the options but to revise the requirement language to reflect that entities should use other options when physical protections cannot be used.

Wednesday, March 19

(Communication Networks continued)

The SDT discussed requirement language on protections for physical input/output ports within the Electronic Security Perimeter (ESP). The SDT stated its intent is to develop language that required protections for devices

within the ESP but do not fall under the definition of a BES Cyber Asset. The SDT determined that the subgroup should address this in the applicability section.

The SDT determined that if a definition is written for communication networks, it should be developed after the FERC technical conference as its outcome may impact the definition.

The SDT developed the following action items for the CN subgroup:

- CIP-006
  - Refine "monitor and respond" language
  - Modify language after informal straw poll
  - Develop guidance on nonprogrammable components
    - Articulate what we are trying to protect
  - In near future, develop rationale boxes
- CIP-007
  - Clarify applicability column
- Definition
- Develop rationale and/or guidance on SDT's direction for addressing directive

10. **Transient Devices (TD)**

The SDT discussed the requirements developed to address the TD directive. The SDT discussed whether authorization of individuals to use Transient Cyber Assets and Removable Media should be included in the requirements. The SDT determined that it would not be feasible to authorize everyone who used a Transient Cyber Asset. The SDT also determined that it needs to consider transient devices with a maintenance function and how to deal with non-entity-managed transient devices.

Based on these discussions, the SDT removed "authorization of individuals" from its proposed requirement because it would be covered under CIP-004-5. Furthermore, the SDT determined that a training component should be added to CIP-004-5 to cover Transient Cyber Assets and Removable Media. The SDT also removed "information protection" from the proposed requirement because it already was covered by CIP-011-1. Finally, the SDT wanted to consider developing a definition for Transient Cyber Assets and Removable Media.

The SDT developed the following action items for the TD subgroup:

- Clarify that CIP-004 covers the training issue
- Address whether we want to restrict tools to individuals
- Draft Consideration of Issues and Directives
- Develop language that gives entity some timeframe flexibility of when entity will do checks
- Consider splitting Removable Media and Transient Cyber Assets for .3
  - Define Removable Media?
  - Per device capability?
  - Avoid requirement redundancies/duplication
- Discuss element 6 from FERC Order (processes and procedures…)
- Develop guidance as specified in comments on latest working document

11. **Low Impact Assets (LIA) Protections**

    The SDT discussed developing objective criteria within the four technical areas within CIP-003-5, Requirement R2, Parts 2.1-2.4. The SDT noted that the revisions were used from other CIP standards for consistency in language. Meeting participants noted that additional guidance for electronic and physical access requirements may be needed.

    The SDT discussed the use of "processes" or "policies" in Requirement R2. The SDT determined that because of the addition of objective criteria, the word "processes" was more appropriate than "policies." The SDT stated that policies are on a higher level than processes, and the objective criteria made the requirements too granular to be considered parts of policies. Therefore, the SDT used processes in CIP-003-5, Requirement R2. The SDT further determined that the CIP Senior Manager approval should not be included in the requirement because the person in that role usually is at a higher level than approving processes.

    The SDT developed the following action items for the LIA subgroup:

    - Address suggestions for draft language
    - Complete the sentence
    - Develop guidance (e.g. 2.1 and 2.2 on controls)
        - Address individuals that may not have electronic access
    - Review "timely"
    - Consider those entities with joint ownership/access

Thursday, March 20

12. **Standards Authorization Request (SAR) Redline**

    NERC staff noted that the SAR revisions were posted on the project page.

13. **Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for submittal to NERC Board**

    NERC staff noted that FERC approved the request for an extension of time to file. The filing deadline is May 15, 2014 for the VRFs.

14. **Implementation Plan**

    The SDT determined that the co-chairs would develop a draft implementation plan and revise it as the requirements language changes.

15. **Other Standards Development Components**

    The SDT reviewed the items that would be posted with the standards during the comment and ballot period. The SDT would work on these items once the requirements language is firmer.

16. **Action Items and Next Steps**

    The SDT discussed potentially holding webinars in April and June.

17. **Discuss Industry Outreach Opportunities**

18. **Review Development Timeline**

19. **Future Meeting Schedules and Venues**

a. April 22-24, NERC (Atlanta, GA) – In-person: Register

- April 22 (9am-5pm ET) – Web: Register
- April 23 (8am-5pm ET) – Web: Register
- April 24 (8am-12pm ET) – Web: Register

b. May 12-14, American Electric Power (Columbus, OH) – In-person: Register

- May 12 (12pm-5pm ET) – Web: Register
- May 13 (8am-5pm ET) – Web: Register
- May 14 (8am-12pm ET) – Web: Register

c. Planning Holds for Q3

20. **Adjourn**