NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02 Standard Drafting Team Conference Calls Notes

March 10, 2014 to March 14, 2014

Full Standard Drafting Team Call – March 10, 2014

Quorum was reached as 9 of the 10 Standard Drafting Team (SDT) members joined the call.

Identify, Assess, and Correct (IAC) Discussion

The IAC leads noted that the previous week's call participants favored the CIP-003-5 example of removal over the CIP-011-1 example of modification of IAC language. As a result, the leads noted they went through the whole suite of CIP standards to remove the IAC language and would discuss this approach on the next subgroup call. They would also discuss the team's ideas on including self-correcting language attribute for the requirements during future calls.

Communication Networks (CN) Discussion

The CN leads discussed their work from the previous week on CIP-006 and CIP-007. They noted that there was general agreement with their approach, but there was still some work on the wording needed. The SDT discussed the issue of regional differences in Electronic Security Perimeters (ESPs), and the leads would have diagrams demonstrating the differences for the subgroup call later in the week.

Transient Devices (TD) Discussion

The TD leads reviewed their work from last week. The subgroup had discussed entity- versus non-entity-managed devices and how to handle them in the standard. The SDT noted that there were still some issues to consider such as renewing devices' pre-authorization, addressing patch management, and handling devices that go from the field to a Control Center system. The SDT stated that the subgroup should keep its focus on protecting the BES when considering these issues.

Low Impact Assets (LIA) Discussion

The LIA leads provided a summary of the actions on last week's call and noted that they are starting to develop language. They mentioned they would like to flesh out the options for placement within the CIP family of standards and determining the SDT's preferred direction before developing language. The SDT noted that the language would likely go into CIP-003-5 Requirement R2 but there are still several options for the language.

Identify, Assess, Correct (IAC) Subgroup Call – March 11, 2014

The IAC leads presented the 17 requirements with IAC language removed. There was discussion regarding the Reliability Assurance Initiative (RAI), and the call participants developed questions to ask NERC compliance and enforcement during the RAI presentation at the face-to-face meeting in Sacramento. The subgroup took the following action items based on the discussion.

Action Items

- Develop questions for the RAI presentation in Sacramento

Communication Networks (CN) Subgroup Call – March 11, 2014

The CN leads presented modifications to CIP-006-5 and CIP-007-5. There was discussion on language, particularly what "protecting" will mean in the context of CIP-006-5. The leads presented diagrams of regional differences in Electronic Security Perimeters (ESPs). Call participants discussed how the proposed applicability will cover the different regional ESPs for both CIP-006-5 and CIP-007-5.

Action items

- Work on detection and response language for CIP-006-5
- Rationale for modifications
- Guidance for CIP-007
- Greg will put PSPs around diagram he sent; Dave R. will put PSP around extended ESP
- NERC will put CIP-006 and CIP-007 into template

Low Impact Assets (LIA) Subgroup Call – March 13, 2014

The LIA leads presented the risk associated with the options discussed in the previous week. Call participants noted that the option to only revise language in CIP-003-5, Requirement R2 for Low Impact assets was the best place to start drafting. The leads then proposed language to include in CIP-003-5, Requirement R2 to address the directive. The proposal included objectives for each of the four technical areas in the original requirement. Call participants discussed the objectives and the language to make the requirement more auditable.

Action items

- Revise language of CIP-003-5, Requirement R2 to address the following considerations:
    - For cyber security awareness, consider incorporating CIP-004-5.1, Requirement R4, Part 4.1, consider using a timeframe, and consider including awareness of Parts 2.2 through 2.4 of CIP-003-5, Requirement R2.

- For physical security controls, consider whether authorization is needed in the language.
- For electronic access controls, consider incorporating CIP-006-5, Requirement 1, Part 1.1.

Transient Devices (TD) Subgroup Call – March 13, 2014

The TD leads proposed a requirement with four requirement parts addressing transient devices protections, but whether the proposal becomes a standard or is incorporated into other CIP standards is still undecided. The leads noted that they used NIST 800-53, MA-3 as a reference. They developed a definition of transient cyber asset, and the proposed requirements addressed device authorization, malicious code prevention, software detection, and prevention of access to BES Cyber System Information. Call participants discussed revisions to the proposed language.

Action items

- Present revised language to full Standard Drafting Team and observers at face-to-face meeting in Sacramento