NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2019-02 BES Cyber System Information Access Management Standard Drafting Team

October 14, 2020 | 1:00 – 3:00 p.m. Eastern
October 15, 2020 | 1:00 – 3:00 p.m. Eastern

Conference Call

Administrative

1. **Introductions**

   J. Hansen (Vice Chair) greeted everyone and reviewed the purpose of the meeting. The following standard drafting team (SDT) members were in attendance:

	Name	Entity	Yes/No
Chair	John Hansen	Exelon	**Y**
Vice Chair	Josh Powers	Southwest Power Pool, Inc. (SPP)	**Y**
Members	Victoria Bethley	Duke Energy	**Y**
	Sharon Koller	American Transmission Company, LLC	**N**
	Michael Lewis	Southern California Edison	**Y**
	Conor Martin	Arizona Public Service	**Y**
	Regan Plain	Minnkota Power Cooperative	**Y**
	Joshua Roper	Westar and KCP&L, Evergy Companies	**Y**
	Clay Walker	Cleco Corporate Holdings LLC	**N**
	William Vesely	Consolidated Edison Company of New York, Inc.	**Y**
NERC Staff	Latrice Harkness – Senior Standards Developer	North American Electric Reliability Corporation	**Y**

	Daniel Bogle – Compliance Assurance	North American Electric Reliability	**Y**
	Marisa Hecht – Legal	North American Electric Reliability Corporation	**Y**

2. **Determination of Quorum**
   The rule for NERC SDT states that a quorum requires two-thirds of the voting members of the SDT to be physically present. Quorum was established as seven of the total members were present.
3. **NERC Antitrust Compliance Guidelines and Public Announcement**
   L. Harkness reviewed the NERC Antitrust Compliance Guidelines and Public Announcement.

Agenda

1. **Industry Comment Review**
   The team provided an overview of the industry comments based on assignment questions. The noted themes and trends are as follows:

   Question 1 (CIP-004)

   - Use of the phrase provisioned access
   - Scope expansion for the 15-month review
   - The name change of the "Applicable Systems" Column
   - Recommendation to include language from the Technical Rationale for clarifying provisioned access
   - Clarification on what is needed for access management

   Question 2 (CIP-004)

   - Security Gap | More Explicitly differentiate between/state protections for physical vs electronic BES Cyber System Information (BCSI) Protections
   - Like the Technical Rationale about "provisioning", but it is not enforceable. Add the Requirement Language for clarity.
   - Do not like the term "provisioning". Define, or provide clarity in requirement language.
   - Leverage the language in the current CMEP Practice Guide. State "access and use" in the requirement instead of just "use". Also, incorporate "Compliance Implementation Guidance Cloud Solutions and Encrypting BES Cyber System Information – June 2020"
   - Go back to designated storage locations

- Remove Requirement R6. Use sample language in SAR to update Requirement R4 Part 4.1. Or better align Requirement R6 with the Technical Rationale.

Question 3 (CIP-011)

- No overview was provided

Question 4 (VRF/VSL)

- VRFs/VSLs did not represent the risk and severity of the Requirements.

Question 5 (Implementation Plan)

- Increase to 24 or 36 months
- Provide more clarity for CIP-011, Requirement R1, Part 1.3

Question 6

- No overview was provided

Question 7

- Continued confusion between CIP-011 Requirement R1 Part 1.3 and CIP-013
- Consistent Redlines. Redline to last posted is different than redline to last approved
- Consistency between Requirement language and Measures
- Applicability confusion from shift of "Applicable Systems" to "Applicability"
- Go back to Storage Locations
- Confusion on the word "use"
- Limit Medium impact to ERC only in CIP-011
- Missing transfer and reassignment requirements. Potential gap.
- General lack of clarity. Want more details in Requirements
- Perceived expansion of scope for 15-month review
- Concern about bare minimum and use of inadequate encryption key strength
- Get rid of CIP Standards and use National Institute of Standards and Technology (NIST)

2. BCSI in the cloud

The SDT discussed what elements are needed for storing BES Cyber System Information in the cloud. Three questions were posed:

How do we control access?

How do we protect information?

What are the actionable steps for the Responsible Entity?

J. Powers asked the team should CIP-004 Requirement R4 be revised or should the SDT modify Requirement R6 to address access to BCSI. Four members recommended keeping Requirement R6. R. Plain stated that it could be addressed in both ways depending on the applicability. It was also stated that the standards haven't hit the mark for managing physical or electronic access to BCSI. Based on industry comment the team needs to clarify access management for physical to physical and electronic to electronic.

3. Draft Revisions Next Steps

J. Hansen shared that based on industry comment CIP-004 Requirement R6 still does not convey the concept of access to BCSI. There needed to be a distinction between people who can access the data and use BCSI (obtain and use) verses people who can obtain and not use BCSI. Some recommendations included removing "authorized access", creating separate sub-requirements for physical and electronic access, and to not conflate the two issues. In order to do this maybe break apart authorization and controlling of access.

The SDT discussed the need for CIP-011 Requirements Part 1.3 and 1.4. It was stated that if the Requirements are deleted then there is a risk that no controls will exist for BCSI stored using vendor services. A FERC observer also posed a question to the SDT, "What is the security objective?" Industry comments still suggest that Part 1.3 and 1.4 will be covered by the assessment required in CIP-013. R. Plain suggested that Requirement R1, Part 1.3. was covered in Part 1.2.

The SDT voted to keep Part 1.3. The results are as follows: Six SDT members voted to keep Part 1.3, one SDT voted to remove. There were three SDT members not present for voting.

The SDT voted to keep Part 1.4. The results are as follows: Four SDT members voted to keep Part 1.4, two SDT voted to remove, and there was one abstention. There were three SDT members not present for voting.

4. Phased Implementation Plan

The SDT discussed the possibility for a phased implementation plan. L. Harkness told the SDT that there would have to be some clear measurable milestones in order to have a phased plan. The SDT is going to revisit after the language is finalized.

5. Action Items

Existing Subgroups were assigned to making revisions to CIP-004 and CIP-011. The subgroups are as follows:

CIP-004	CIP-011
J. Powers	J. Hansen
R. Plain	J. Roper
C. Martin	W. Vesely

V. Bethley	C. Walker
S. Koller	M. Lewis

6. **Future Meetings**

7. **Adjourn**
   The meeting adjourned at 2:41 p.m. Eastern on October 15, 2020.