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

February 25-26 | 8:30 a.m. – 4:00 p.m. Central
February 27, 2020 | 8:30 a.m. – 12:00 p.m. Central

Conference Call

Administrative

1. **Introductions**

   J. Hansen (Vice Chair) greeted everyone and thanked CPS Energy for hosting 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
	Andrew Camargo	San Diego Gas & Electric	Y
	Sharon Koller	American Transmission Company, LLC	Y
	Michael Lewis	Southern California Edison	Y
	Conor Martin	Arizona Public Service	Y
	Yoel Piney	PSEG	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

PMOS Liaison(s)	Colby Bellville	Cooperative Energy	Y
	Kirk Rosener	CPS Energy	N
NERC Staff	Latrice Harkness – Senior Standards Developer	North American Electric Reliability Corporation	N
	Daniel Bogle – Compliance Assurance	North American Electric Reliability	N
	Marisa Hecht – Legal	North American Electric Reliability	N
	Lauren Perotti – Legal	North American Electric Reliability Corporation	N

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 achieved as eleven 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. **Response to Comments**
The team reviewed industry comment for CIP-004 and CIP-011. Team members shared comment themes for each questions. Comment themes included revising to include objective based Requirements verses being prescriptive, concerns about the vendor risk assessment and overlap with CIP-013 Requirements, transferal of BES Cyber System Information (BCSI) access requirement to CIP-011, clarification on key management requirements, and clarification of BCSI access. The team also noted concerns possible "double jeopardy" for access revocation.

2. **Draft Standards**
J. Hansen made a motion to move CIP-011 Requirements R1, Parts 1.3, 1.5, and 1.6 back to CIP-004. C. Martin seconded the motion. The motion was approved with nine affirmative votes. There were three abstentions. The SDT discussed an issue concerning managing physical access to electronic access (repositories) when using a third party. Industry suggested a definition of "BCSI Repository" to clarify location with respect to electronic storage locations. The team decided to continue focusing on protection of the information and not the locations.

J. Power made a motion to remove PCA access management in CIP-004 and J. Roper seconded. The motion was approved.

The team also discussed proposed revisions to CIP-011 Requirement R1, Part 1.X about the vendor risk assessment language. Some commenter said that the risk assessment should be a part of CIP-013 and that "the SDT should consider creating a requirement to develop and implement a BCSI security risk assessment plan and describe the criteria that should be included in the plan (for example, a process to authorize access, a process to prevent ability to obtain and use BCSI from unauthorized access, a process to revoke access within the next calendar day, etc.). This approach allows an Entity:

- o to focus on identifying information security risks and objectives specific to its needs and appropriately addressing them;

- o flexibility and scalability regarding how to implement technical controls, as well as remediation and mitigation activities; and

- o the ability to leverage emerging technologies that might better address information security risks without requiring updates to CIP Reliability Standards."

The SDT discussed, and it was stated that when drafting the Requirements the focus should be on the vendor environment and not the vendor. In addition, the SDT consulted with the Project 2019-03 SDT leadership about the overlap with CIP-013 required assessment and the use of the work "mitigate." The 2019-03 leadership felt that this assessment was already being performed as required by CIP-013. The 2019-02 SDT rebutted that the CIP-013 assessment was focused on procurement of BES Cyber Assets. After the discussion, the 2019-02 SDT drafted some proposed language that requires implementation of risk management method(s) for data governance and rights management, identity and access management, security management, and application, infrastructure and network security. This language was presented to the 2019-03 leadership as well as participating active observers. During the initial review, no one had any issues with the language.

3. **Next Steps**

   a. The team will continue working on assignments for the next posting.

4. **Project Timeline**

   L. Harkness reviewed the timeline with the SDT.

5. **Future Meetings**

   a. March 11, 2020

   b. March 17-19, 2020 | Face-to-Face | SPP

6. **Adjourn**
   The meeting adjourned at 12:33 p.m. Central on February 27, 2020.