NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

June 17, 2020 | 1:00 – 3:00 p.m. Eastern
June 18, 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	**N**
	Sharon Koller	American Transmission Company, LLC	**Y**
	Michael Lewis	Southern California Edison	**N**
	Conor Martin	Arizona Public Service	**Y**
	Regan Plain	Minnkota Power Cooperative	**Y**
	Joshua Roper	Westar and KCP&L, Evergy Companies	**N**
	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**
	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 not established as six 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. **Quality Review Feedback**
   The team reviewed the proposed VSLs for CIP-004 Requirement R6 and CIP-011 Requirement R1 (see Attachment 1). The team decided to simplify the VSLs and use language from CIP-005 to draft proposed VSLs. The SDT continued to review the feedback from the quality review period and made revisions as necessary.

   The team reviewed feedback for CIP-011 Requirement R1, Part 1.3 regarding vendor services. The SDT discussed potential revisions to clarify and assess the risk of using vendor services for BES Cyber System Information. Many industry comments stated that there was an overlap between this Requirement sub-part and CIP-013 assessment. A sub-team was formed to draft some proposed language to address the concern.

   The team did not review the Implementation Plan during this meeting.
2. **SDT Assignments**
   J. Hansen encouraged the team to continue working on the supporting documentation as assigned. No action taken.
3. **Future Meetings**
   a. June 24, 2020 | 1:00 – 3:00 p.m. Eastern
4. **Adjourn**
   The meeting adjourned at 2:57 p.m. Eastern on June 18, 2020.

Attachment 1

CIP-004 Violation Severity Level (VSL)

Requirement R6

Option 1

Lower VSL

The Responsible Entity has implemented one or more documented access management program(s) for BES Cyber System Information, but one of the following issues occurred:

The Responsible Entity authorized an individual's access to BES Cyber System Information within 30 calendar days after the access was provisioned. (6.1)

OR

The Responsible Entity verified within 16 calendar months from the previous verification that all provisioned access to BES Cyber System Information is authorized and is appropriate based on need, as determined by the Responsible Entity. (6.2)

OR

For a termination action, the Responsible Entity did not remove one individual's ability to use provisioned access to BES Cyber System Information (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action. (6.3)

Moderate VSL

The Responsible Entity has implemented one or more documented access management program(s) for BES Cyber System Information, but one of the following issues occurred:

The Responsible Entity authorized an individual's access to BES Cyber System Information within 90 calendar days after the access was provisioned. (6.1)

OR

The Responsible Entity verified within 17 calendar months from the previous verification that all provisioned access to BES Cyber System Information is authorized and is appropriate based on need, as determined by the Responsible Entity. (6.2)

OR

For termination actions, the Responsible Entity did not remove two individuals' ability to use provisioned access to BES Cyber System Information (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective dates of the termination actions. (6.3)

Option 2

Lower VSL

The Responsible Entity implemented one or more documented access management program(s) for BES Cyber System Information but did not implement one of the requirements found in Parts 6.1 through 6.3. (R6)

Moderate VSL

The Responsible Entity implemented one or more documented access management program(s) for BES Cyber System Information but did not implement two of the requirements found in Parts 6.1 through 6.3. (R6)

High VSL

The Responsible Entity implemented one or more documented access management program(s) for BES Cyber System Information but did not implement three or more of the requirements found in Parts 6.1 through 6.3. (R6)

Severe VSL

The Responsible Entity did not implement one or more documented access management program(s) for BES Cyber System Information. (R6)

CIP-011 Violation Severity Level (VSL)

Requirement R1

Option 1

Lower VSL

The Responsible Entity implemented one or more documented information protection program(s), and the Responsible Entity implemented a method(s) to prevent unauthorized access to BES Cyber System Information, but the Responsible Entity disclosed BES Cyber System Information to one or more employees of the Responsible Entity who were not authorized to access BES Cyber System Information. (1.2)

Moderate VSL

The Responsible Entity implemented one or more documented information protection program(s), and the Responsible Entity implemented a method(s) to prevent unauthorized access to BES Cyber System Information, but the Responsible Entity disclosed BES Cyber System Information to one or more third parties who were not authorized to access BES Cyber System Information. (1.2)

High VSL

The Responsible Entity implemented one or more documented information protection program(s), but one of the following issues occurred:

The Responsible Entity did not implement a method(s) to identify information that meets the definition of BES Cyber System Information. (1.1)

OR

The Responsible Entity did not implement a method(s) to prevent unauthorized access to BES Cyber System Information. (1.2)

OR

When the Responsible Entity used a vendor's services for BES Cyber System Information, the Responsible Entity did not implement a risk management method(s) for data governance and rights management; identity and access management; security management; or application, infrastructure, and network security. (1.3)

Severe VSL

The Responsible Entity did not implement one or more documented information protection program(s). (R1)

Option 2

Lower VSL

The Responsible Entity implemented one or more documented information protection program(s) but did not implement one of the requirements found in Parts 1.1 through 1.3.4. (R1)

Moderate VSL

The Responsible Entity implemented one or more documented information protection program(s) but did not implement two of the requirements found in Parts 1.1 through 1.3.4. (R1)

High VSL

The Responsible Entity implemented one or more documented information protection program(s) but did not implement three or more of the requirements found in Parts 1.1 through 1.3.4. (R1)

Severe VSL

The Responsible Entity did not implement one or more documented information protection program(s). (R1)

Requirement R2

Option 1

Lower VSL

When the Responsible Entity used a vendor's services for BES Cyber System Information, the Responsible Entity implemented one or more electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information, but the Responsible Entity disclosed BES Cyber System Information to one or more employees of the Responsible Entity who were not authorized to access BES Cyber System Information.

Moderate VSL

When the Responsible Entity used a vendor's services for BES Cyber System Information, the Responsible Entity implemented one or more electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information, but the Responsible Entity disclosed BES Cyber System Information to one or more employees of the vendor who were not authorized to access BES Cyber System Information.

High VSL

When the Responsible Entity has used a vendor's services for BES Cyber System Information, the Responsible Entity has documented one or more electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information but has not implemented electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information.

Severe VSL

When the Responsible Entity used a vendor's services for BES Cyber System Information, the Responsible Entity did not implement electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information.

Option 2

Lower VSL

N/A

Moderate VSL

N/A

High VSL

When the Responsible Entity used a vendor's services for BES Cyber System Information as identified in Requirement R1, Part 1.1, the Responsible Entity documented one or more electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information but did not implement electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information. (R2)

Severe VSL

When the Responsible Entity used a vendor's services for BES Cyber System Information as identified in Requirement R1, Part 1.1, the Responsible Entity did not implement electronic technical mechanisms to prevent unauthorized logical access to BES Cyber System Information. (R2)