NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2019-02 BES Cyber System Information Access Management

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2019-02 BES Cyber System Information Access Management** by **8 p.m. Eastern, Monday, May 10, 2021.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

Background Information

The purpose of Project 2019-02 BES Cyber System Information Access Management is to clarify the CIP requirements related to both managing access and securing BES Cyber System Information (BCSI). This project proposes revisions to Reliability Standards CIP-004-6 and CIP-011-2.

The proposed revisions enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BCSI. In addition, the proposed revisions clarify the protections expected when utilizing third-party solutions (e.g., cloud services).

Questions

1. The standards drafting team (SDT) considered industry's concerns about the phrase "provisioning of access" requesting clarity on this terminology. The SDT added "authorize, verify, and revoke provisioned access" to the parent requirement CIP-004-X, Requirement R6, and changed "provisioning of access" to "provisioned access" in the requirement parts. This should clarify the intent that it is a noun which scopes what the Registered Entity must authorize, verify, and revoke, rather than a verb relating to how provisioning should occur. That is up to the entity to determine. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   We support these changes.

2. The SDT considered industry's concerns about the absence of "obtain and use" language from the CMEP Practice Guide, which currently provides alignment on a clear two-pronged test of what constitutes access in the context of utilizing third-party solutions (e.g., cloud services) for BCSI. The SDT mindfully mirrored this language to assure future enforceable standards are not reintroducing a gap. Do you agree this clarifying language makes it clear both parameters of this two-pronged test for "obtain and use" must be met to constitute "access" to BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   We support the update to this Requirement language.

3. The SDT considered industry comments regarding the removal of storage locations. The SDT must enable the CIP standards for the use of third-party solutions (e.g., cloud services) for BCSI, and retention of that language hinders meeting those FERC directives. The absence of this former language does not preclude an entity from defining storage locations as the method used within an entity's access management program. CIP-004-X, Requirement R6, is at an objective level to permit more than that one approach. Do you agree the requirement retains the flexibility for storage locations to be used as one way to meet the objective? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   If the entity continues using storage location, the entity is responsible for defining storage location. Request confirmation of this expectation.

4. To address industry comments while also enabling entities to use third-party solutions (e.g., cloud services) for BCSI, in CIP-004-X, Requirement R6 Part 6.1, the SDT made a distinction between "electronic access to electronic BCSI" versus "physical access to physical BCSI". This clarifies physical access alone to hardware containing electronic BCSI, which is protected with methods that do not permit an individual to concurrently obtain and use the electronic BCSI, is not provisioned access to electronic BCSI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

5. The SDT considered industry comments about defining the word “access”. “Access” is broadly used across both the CIP and Operations & Planning Standards (e.g., open access) and carries different meanings in different contexts. Therefore, the SDT chose not to define “access” in the NERC Glossary of Terms. Instead, the SDT used the adjective “provisioned” to add context, thereby scoping CIP-004-X, Requirement R6. Do you agree the adjective “provisioned” in conjunction with the “Note” clarifies what “provisioned access” is? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   We agree that the Note clarifies provisioned access.

   We have concerns – 1) as written the reference to Part 4.1 could result in double jeopardy; 2) request clarification on how granting access in Part 4.1 could provide authorization to BCSI required in Part 6.1

6. In response to industry concerns regarding double jeopardy or confusion with CIP-013, the SDT removed CIP-011-X, Requirement R1 Parts 1.3 and 1.4, in favor of simplifying CIP-011-X, Requirement R1 Part 1.1, and adjusting Part 1.2 to broaden the focus around the implementation of protective methods and secure handling methods to mitigate risks of compromising confidentiality. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   We agree with this simplification.

7. The SDT extended the implementation plan to 24-months in an attempt to align with the Project 2016-02 modifications that are on the same drafting timeline, and added an optional provision for early adoption. Do you agree this approach gives industry adequate time to implement without encumbering entities who are planning to, or are already using, third-party solutions (e.g., cloud services) for BCSI? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   We agree with aligning timelines.

8. In looking at all proposed recommendations from the standard drafting team, are the proposed changes a cost-effective approach?
   - ☐ Yes
   - ☐ No

   Comments:

9. Please provide any additional comments for the SDT to consider, if desired.

   Comments:

   Request clarification on Part 6.2's Measures. Will auditing/enforcement expect every item? This Measure starts with "Examples of evidence may include." Does the SDT mean this "may" is a "shall?" Recommend changing "Examples" to "Example."

   We look forward to seeing the final combined version of this update and the virtualization update.