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)](https://sbs.nerc.net/) to submit comments on **Project 2019-02 BES Cyber System Information Access Management** by **8 p.m. Eastern, February 3, 2020.**

Additional information is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project2019-02BCSIAccessManagement.aspx). If you have questions, contact Senior Standards Developer, Latrice Harkness (via email), or at 404-446-9728.

## 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, including moving some existing CIP-004-6 Requirements to proposed CIP-011-3.

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 proposed revision to Requirement R1 Part 1.1 adds the requirement to identify BCSI storage locations. Do you agree that the requirement as written allows the Responsible Entity the flexibility to identify which storage locations are for BCSI? Do you agree the requirement is necessary? If you disagree with the changes made, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

[ ]  Yes

[ ]  No

Comments:

1. The standard drafting team (SDT) attempted to maintain backwards compatibility with concepts of designated storage locations and access-level requirements previously contained in CIP-004-6. Do you agree that there is a minimal effort to meet this objective while providing greater clarity between BCSI and BES Cyber System (BCS) requirement obligations?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is attempting to expand information storage solutions or security technologies for Responsible Entities. Do you agree that this approach is reflected in the proposed requirements?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is addressing, and further defining, the risk regarding potential compromise of BCSI through the inclusion of the terms “obtain” and “use” in requirement CIP-011-3, Requirement R1 Part 1.2. Do you agree that this will more accurately address the risk related to the potential compromise of BCSI versus the previous approach?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to have BCSI in the “Applicability” column. Do you agree that this provides better clarity on the focus of the requirements?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to address the security risks associated with BCSI environments, particularly owned or managed by vendors via CIP-011-3, Requirements R1, Part 1.4, and Requirement R2, Parts 2.1 and 2.2. Do you agree that these requirements will promote a better understanding of security risks involved while also providing opportunities for the Responsible Entity to address appropriate security controls?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is addressing the growing demand for Responsible Entities to leverage new and future technologies such as cloud services. Do you agree that the proposed changes support this endeavor?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing a new “key management” set of requirements. Do you agree that key management involving BCSI is integral to protecting BCSI?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to shift the focus of security of BCSI more towards the BCSI itself rather than physical security or “hardware” storage locations. Do you agree that this approach aids the Responsible Entity by reducing potential unneeded controls on BCS?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to transfer all BCSI-related requirements from CIP-004 to CIP-011 with the understanding that this will further address differing security needs between BCSI and BCS as well as ease future standard development. Do you agree that this provides greater clarity between BCSI and BCS requirements?

[ ]  Yes

[ ]  No

Comments:

1. The SDT increased the scope of information to be evaluated by including both Protected Cyber Assets and all Medium Impact (not just Medium Impact Assets with External Routable Connectivity). Are there any concerns regarding a Responsible Entity attempting to meet these proposed, expanded requirements?

[ ]  Yes

[ ]  No

Comments:

1. In looking at all proposed recommendations from the SDT, are the proposed changes a cost-effective approach?

[ ]  Yes

[ ]  No

Comments:

1. Do you have any other general recommendations/considerations for the drafting team?

[ ]  Yes

[ ]  No

Comments: