Unofficial Comment Form
Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on CIP-012-1 – Cyber Security – Communications between Control Centers. Comments must be submitted by 8 p.m. Eastern, Monday, December 11, 2017.

Additional information is available on the project page. If you have questions, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

Background Information
On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to “develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).” (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements allowing Responsible Entities to apply protection to the links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity’s operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.
Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments:
We are still unclear on the included data. For R1.2, recommend that the Entities should mutually agree on the demarcation points. For R1.3, we are concerned with resolution of disagreements between different Entities.

2. Requirement R1: The SDT seeks comment on scoping sensitive BES data as it applies to Real-time Assessment and Real-time monitoring and control data. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

☒ Yes
☐ No

Comments:
We conceptually agree with the scoping but need more details on “monitoring and control data.” We agree with the removal of “Operational Planning Analysis.”

3. Requirement R2: The SDT drafted CIP-012-1 Requirement R2 for the Responsible Entity to implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

4. Implementation Plan: The SDT revised the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority’s order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.
Comments:
We are concerned about equipment under existing contracts. We suggest a solution similar to CIP-013.

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Comments:
Cost effectiveness will be determined by the Entity’s implementation and existing contracts.

6. If you have additional comments on the proposed CIP-012-1 – Cyber Security – Communications between Control Centers drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Comments:
Removal of the SDT’s Guidance and Technical Basis (GTB) from the Standard makes it difficult to 1) understand the intent and 2) evaluate this version. If the GTB is not restored, we recommend posting the GTB information simultaneous with the Standard.