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, April 30, 2018.

Additional information is available on the project page. If you have questions, contact Jordan Mallory at (404) 446-2589 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 CIP-012-1 allowing Responsible Entities to apply protection to the links, the data, or both, in order to satisfy the security objective consistent with the capabilities of the Responsible Entity’s operational environment. Requirement R1 requires Responsible Entities to implement one or more document plans that protect Real-time Assessment and Real-time monitoring 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.
Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring 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:

2. Implementation Plan: The SDT established 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.

☐ Yes
☐ No

Comments:

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT’s intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

☐ Yes
☐ No

Comments:

Recommend removing the diagram because it does not represent enough examples. We believe the scope is understandable without the diagram.
4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC’s Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☒ No

Comments:

Request a definition of “logical protection” or replace all instances of “logical protection” with “encryption”

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.

☒ Yes
☐ No

Comments: