Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards  
CIP-012-1

**Do not** use this form for submitting comments. Use the [electronic form](https://sbs.nerc.net/) to submit comments on  
**CIP-012-1 - Cyber Security – Control Center Communication Networks.** The electronic form must be submitted by **8 p.m. Eastern, Monday, September 11, 2017.  
m. Eastern, Thursday, August 20, 2015**

Additional information is available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx). If you have questions, contact Standards Developers, [Katherine Street](mailto:katherine.street@nerc.net) (404-446-69702) or [Mat Bunch](mailto:mat.bunch@nerc.net) (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 and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards, 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 Operational Planning Analysis, 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. Requirement R2 covers implementation of the plan developed according to Requirement R1.

## Questions

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

Yes

No

Comments:

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

Yes

No

Comments:

1. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) 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 agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Yes

No

Comments:

1. 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:

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

Comments: