Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

CIP-003-8

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System](https://sbs.nerc.net/) to submit comments on **CIP-003-8 - Cyber Security – Security Management Controls (FERC Order No. 843 – Third Party TCA)**. Comments must be submitted by **8 p.m. Eastern, Tuesday, October 9, 2018.
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 Developer, Jordan Mallory (via email) or at 404-446-2589.

## Background Information

On April 19, 2018, the Commission issued Order No. 843, approving CIP-003-7 and directing a modification to CIP-003-7 related to the mitigation of risk associated with the use of third-party transient electronic devices. The Commission directed NERC to “develop and submit modifications to Reliability Standard CIP-003-7 to include an explicit requirement that Responsible Entities implement controls to mitigate the risk of malicious code that could result from third-party transient electronic devices.”

## SDT Approach

The Project 2016-02 Standard Drafting Team (SDT) revised Reliability Standard CIP-003-7 to require Responsible Entities to determine whether additional mitigation is necessary to address the risk of the introduction of malicious code to low impact BES Cyber Systems when using third-party Transient Cyber Assets. The revision also requires that Responsible Entities implement any mitigation prior to connecting the Transient Cyber Asset. The SDT based this additional determination and implementation step for third-party Transient Cyber Assets on the currently approved language in CIP-010-2, Attachment 1 for the use of Transient Cyber Assets with high and medium impact BES Cyber Systems.

## Questions

1. Requirement R2, Attachment 1, Section 5.2: In response to the directive in FERC Order 843, the SDT modified Attachment 1, Section 5.2 adding subsection 5.2.2 to state: “For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.” Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. Guidelines and Technical Basis: The SDT made changes to the Guidelines and Technical Basis section of the Standard to conform with the modifications it made to Attachment 1, Section 5.2. Do you agree with these changes to the Guidelines and Technical Basis? If not, please provide the basis for your disagreement and an alternate proposal. (The CIP SDT is aware that another initiative is underway to convert all GTB sections to Technical Rationale documents. This effort is outside the scope of this SDT.)

[ ]  Yes

[ ]  No

Comments:

1. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the later of (1) January 1, 2020, or (2) the first day of the first calendar quarter that is six (6) 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 effective date is needed, please provide a detailed explanation of actions and time needed.

[ ]  Yes

[ ]  No

Comments:

1. The SDT believes proposed modifications in CIP-003-8 provide 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 or procedural justification.

[ ]  Yes

[ ]  No

Comments: