Unofficial Comment Form

# Project 2016-02 Modifications to CIP Standards

Requirements for Transient Cyber Assets – CIP-003-7(i)

**Do not** use this form for submitting comments. Use the [electronic form](https://sbs.nerc.net/) to submit comments
on the **Modifications to address the Federal Energy Regulatory Commission (FERC or the Commission) directive regarding the mandatory protection for transient devices used at Low Impact BES Cyber Systems.** The electronic form must be submitted by **8 p.m. Eastern, Wednesday, January 25, 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 Senior Standards Developer, Al McMeekin at (404) 446-9675.

**Description of Current Draft**

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued [Order No. 822](https://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf), approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified definitions to be incorporated into the Glossary of Terms Used in NERC Reliability Standards. In addition to approving the seven CIP Reliability Standards, the Commission, directed NERC to, among other things,: (1) “…develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems…”, and (2) modify the definition of LERC. On March 9, 2016, the NERC Standards Committee authorized the Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the 2016-02 Modifications to CIP Standards Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

In Order 822, the Commission stated:

32. After consideration of the comments received on this issue, we conclude that the adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. Accordingly, we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission’s concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.

The SDT revised Attachment 1 of CIP-003-7 to require the mitigation of risk to the BES of malware propagation from transient devices to low impact BES Cyber Systems. Attachment 1 contains and outlines the required sections of a Responsible Entity’s cyber security plan(s) for its low impact BES Cyber Systems per Requirement R2. Previously, cyber security plan(s) were required to address four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security Incident response. In keeping with the stakeholder approved approach to incorporate into one standard all the requirements applicable to assets containing low impact BES Cyber Systems, the SDT expanded CIP-003-7 Attachment 1 to include a fifth area: “Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation.” Requiring the Responsible Entity to develop and implement these plans will provide mitigation for malware propagation to BES Cyber Systems from transient devices.

In addition, the SDT determined it was necessary to revise the definitions of a Transient Cyber Asset (TCA) and Removable Media to ensure applicability of security controls and provide additional clarity. As well, the revised definitions accommodate use of the terms for all impact levels: high, medium and low. This is important for those entities that may opt to deploy one program to manage TCAs and Removable Media across multiple impact level assets.

The proposed definition of a Transient Cyber Asset (TCA) is:

*A Cyber Asset that is:*

*1. capable of transmitting or transferring executable code,*

*2. not included in a BES Cyber System,*

*3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and*

*4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:*

* *BES Cyber Asset,*
* *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
* *PCA associated with high or medium impact BES Cyber Systems.*

*Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.*

The proposed definition of Removable Media is:

*Storage media that:*

1. *are not Cyber Assets,*
2. *are capable of transferring executable code,*
3. *can be used to store, copy, move, or access data, and*
4. *are directly connected for 30 consecutive calendar days or less to a:*
	* *BES Cyber Asset,*
	* *network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or*
	* *Protected Cyber Asset associated with high or medium impact BES Cyber Systems.*

*Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.*

As proposed, Section 5 of Attachment 1 of CIP-003-7(i) mandates that entities have malware protection for Transient Cyber Assets (both entity and vendor-managed) and Removable Media. The SDT proposes that it is necessary to distinguish between the specific protections for: (i) Transient Cyber Assets managed by the Responsible Entity, (ii) Transient Cyber Assets managed by a party other than the Responsible Entity (e.g. vendors or contractors), and (iii) Removable Media.

For Transient Cyber Assets managed by the Responsible Entity, Section 5 requires the Responsible Entity to use one or a combination of the following to mitigate the introduction of malicious code: antivirus software, application whitelisting, or some other method. The SDT recognized that entities manage these devices in two fundamentally different ways. Some entities maintain a preauthorized inventory of transient devices (i.e., manage in an ongoing manner) while others have a checklist for transient devices prior to connecting them to a BES Cyber System (i.e., manage in an on-demand manner). The SDT acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher frequency in which these entity-managed devices are used, the controls required for these devices are more specific.

For Transient Cyber Assets managed by a party other than the Responsible Entity, Section 5 requires the Responsible Entity to review and verify the malware mitigation mechanism(s) used by the third party prior to connecting the Transient Cyber Asset (per Transient Cyber Asset capability).

For Removable Media, Section 5 requires entities to employ method(s) to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.

In summary, the SDT made the following changes to address the directive:

1. Revised the definitions of Transient Cyber Asset and Removable Media.
2. Revised Requirement R1, by adding Parts 1.2.5 and 1.2.6 to include the complementary policies for the Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation in Requirement R2 (Attachment 1 of CIP-003-7(i)).
3. Revised the requirement language (Requirement R2) in Attachment 1 of CIP-003-7(i) by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation.
4. Revised the associated VSLs for Requirement R2 of CIP-003-7(i).
5. Revised the evidential language of Attachment 2 of CIP-003-7(i) by adding Section 5 - Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to complement the revised requirement language.

**Development Plan for LERC and TCA Modifications**

The CIP Modifications Standard Drafting Team is currently addressing eight issue areas within the CIP standards including two FERC directed issue areas that directly impact the requirements for low impact BES Cyber Systems - the Low Impact External Routable Connectivity (LERC) modifications and requirements for TCAs used at assets containing low impact BES Cyber Systems. The LERC modifications have a regulatory filing deadline of March 31, 2017. Through outreach, stakeholders have expressed a preference for the SDT to consolidate, as much as possible, proposed changes to the standards that pertain to assets containing low impact BES Cyber Systems and to do so expeditiously. The consolidation would foster stability in the low impact requirements and enable efficient implementation of the requirements which is important given the volume of in-scope assets and the work currently underway for CIP-003-6. Consequently, the SDT and NERC staff are exploring opportunities to accomplish this objective.

This posting combines the language from the successful ballot of CIP-003-7 (Low Impact External Routable Connectivity (LERC) modifications) and the language from the informal posting of CIP-003-TCA (transient devices at low impact modifications) along with revisions based on stakeholder feedback. A successful ballot of CIP-003-7(i) will permit the SDT to complete a final ballot of the combined LERC and TCA language prior to the FERC deadline for the LERC modifications of March 31, 2017.

The SDT is seeking feedback on the draft TCA requirements in CIP-003-7(i). The TCA proposal uses a subset of the language from the CIP-010 TCA requirements commensurate with the risk associated at low impact BES Cyber Systems. The CIP-003-7(i) language is consistent with the existing TCA language for Medium and High Impact BES Cyber Systems to enable a common understanding of the requirements, particularly for those entities implementing a plan to cover high, medium and low impact.

Receiving thoughtful and constructive feedback from stakeholders is critical to the success of this plan. Submitting comments in advance of the deadline is welcome. The SDT thanks you for your participation.

**Questions**

1. Definition: The SDT revised the definition of Transient Cyber Asset such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

Comments:

1. Definition: The SDT revised the definition of Removable Media such that it is relevant to the controls required for high impact, medium impact, and low impact BES Cyber Systems. Do you agree with these changes? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

Comments:

1. Requirement R2: The SDT revised CIP-003-7(i), Attachment 1, adding Section 5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation to reflect the mandatory requirement for the Responsible Entity to develop and implement security plans to mitigate the risk of propagation of malware from transient devices. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

Comments:

1. Attachment 2: The SDT revised the evidential language of CIP-003-7(i), Attachment 2, Section 5 to make the Measures consistent with the requirement language. Do you agree with these revisions? If not, please provide the basis for your disagreement and an alternate proposal.

Yes:

No:

Comments:

1. Guidelines and Technical Basis: The SDT revised the Guidelines and Technical Basis (GTB) section of the standard to reflect the changes made to Requirement R2. The GTB provides support for the technical merits of the requirement and provides examples of temporarily connected devices, and strategies to consider in developing the Transient Cyber Asset and Removable Media malicious code mitigation plan(s) at a conceptual level. Do you agree with the content of the GTB? If not, please provide the basis for your disagreement and alternate or additional proposal(s) for SDT consideration.

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 eighteen (18) 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 undertake that necessitate 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. If you have additional comments on the proposed revisions to address the FERC directive regarding TCAs for low impact BES Cyber Systems that you have **not** provided in response to the questions above, please provide them here.

Comments: