NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Issues and Directives

Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
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.	FERC Order 822, Paragraph 32; issued January 21, 2016	The Project 2016-02 Standard Drafting Team (SDT) revised Attachment 1 of CIP-003-7(i) to mitigate the risk to the BES of malware propagation to low impact BES Cyber Systems from transient devices. 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 all the requirements applicable to assets containing low impact BES Cyber Systems into one standard, 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 higher assurance against the propagation of malware from transient devices. The plan approach for TCAs and Removable Media is consistent with the existing requirement

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		structure applicable to lows and accommodates the risk level of the assets. Additionally, the SDT revised the definitions of Transient Cyber Asset (TCA) and Removable Media. The revised definitions ensure the applicability of security controls, provide clarity, and accommodate the use of the terms for all impact levels: high, medium and low. The revised definitions will allow entities to deploy one program to manage TCAs and Removable Media across multiple impact levels. The revised 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 containing high or medium impact BES Cyber Systems, or

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		• 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 revised 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 Service 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

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		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 on Transient Cyber Assets (both entity and vendor-managed) and for Removable Media. The SDT determined that it was 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 Responsible Entities 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 recognizes that Responsible 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 drafting team acknowledges both methods are effective and Section 5 permits either form of management. Because of the higher

Project 2016-02 Modifications to CIP Standards		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		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 methods to detect malicious code and mitigate the threat of detected malicious code prior to connecting to a low impact BES Cyber System.