NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-003-7 - Cyber Security – Security Management Controls

Requested Approvals

- Reliability Standard CIP-003-7(i) - Cyber Security – Security Management Controls
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Requested Retirements

- Reliability Standard CIP-003-6 - Cyber Security – Security Management Control
- Definition Low Impact BES Cyber System Electronic Access Point (LEAP)
- Definition of Low Impact External Routable Connectivity (LERC)
- Definition of Transient Cyber Asset (TCA)
- Definition of Removable Media

Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, 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 (NERC Glossary). In addition to approving the seven CIP Reliability Standards, the Commission, among other things, directed NERC to: (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 in the NERC Glossary.

With respect to the transient devices directive, 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.

For the LERC directive, the Commission stated:

> 73. Based on the comments received in response to the NOPR, the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule. We agree with NERC and other commenters that a suitable means to address our concern is to modify the Low Impact External Routable Connectivity definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

To address these directives, NERC modified Reliability Standard CIP-003. In responding to the transient devices directive, NERC modified the definitions of 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.

Further, as an alternative to modifying the LERC definition, the standard drafting team retired the terms "LERC" and "LEAP", incorporating those concepts within the requirement language.

General Considerations

This Implementation Plan does not modify the effective date for CIP-003-6 in the Implementation Plan associated with CIP-003-6 nor any of the phased-in compliance dates included therein except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7(i), provided in this Implementation Plan.

Further, this Implementation Plan clarifies that under Requirement R2 of CIP-003-7(i), the Responsible Entity shall not be required to include in its cyber security plan(s) any elements related to Sections 2, 3, and 5 of Attachment 1 until the effective date of CIP-003-7(i). Upon the effective date of CIP-003-7(i), the Responsible Entity's cyber security plan(s) must include the elements required by Sections 2, 3, and 5 of Attachment 1 and the Responsible Entity must implement the controls included in its plan to meet the objectives of Sections 2, 3, and 5.

Effective Dates

The effective dates for the proposed Reliability Standard and NERC Glossary terms are provided below.

Reliability Standard CIP-003-7(i)

Where approval by an applicable governmental authority is required, Reliability Standard CIP-003-7(i) shall become effective on 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.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-003-7(i) shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC Glossary Definitions of Transient Cyber Asset and Removable Media

Where approval by an applicable governmental authority is required, the definitions of Transient Cyber Asset and Removable Media shall become effective on 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 definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definitions of Transient Cyber Asset and Removable Media shall become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the date that the definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Planned or Unplanned Changes

Planned or Unplanned Changes Resulting in a Higher Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-5 titled Planned or Unplanned Changes Resulting in a Higher Categorization.[1]

Unplanned Changes Resulting in Low Impact Categorization – This Implementation Plan incorporates by reference the section in the Implementation Plan associated with CIP-003-6 titled Unplanned Changes Resulting in Low Impact Categorization. That section provides:

> For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System.

Retirement Date

Reliability Standard CIP-003-6

Reliability Standard CIP-003-6 shall be retired immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

Current NERC Glossary of Terms Definition(s) of LERC, LEAP, TCA and Removable Media

The current definitions of LERC and LEAP shall be retired from the NERC Glossary immediately prior to the effective date of Reliability Standard CIP-003-7(i) in the particular jurisdiction in which the revised standard is becoming effective.

The current definitions of Transient Cyber Asset and Removable Media shall be retired from the NERC Glossary immediately prior to the effective date of the revised definitions for those terms in the particular jurisdiction in which the revised definitions are becoming effective.

[1] Due to the length of that section, it is not reproduced herein.