NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Virtualization | Draft 4

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the "CIP Definitions Posting Document (Project 2016-02)"

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the "Revised CIP Standards and Definitions" within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems

- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards and Definitions" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media

- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.