NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

January 23, 2015

This Implementation Plan for the Reliability Standards developed as part of Project 2014-02 CIP Version 5 Revisions replaces the Implementation Plan for the versions of those CIP Reliability Standards adopted by the NERC Board of Trustees on November 13, 2014.

Requested Approvals[+]

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[*]
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[*]
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

[+] During development, Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were balloted as CIP-003-7, CIP-004-7, CIP-007-7, CIP-10-3, and CIP-011-3. Because these Reliability Standards replace versions of these Reliability Standards adopted by the Board in November 2014 using version numbers -6 and -2, which have not been filed with applicable governmental authorities, the version numbers will revert back to -6 and -2 for purposes of Board adoption and filing with applicable governmental authorities.

[*] The NERC Board of Trustees adopted Reliability Standards CIP-006-6 and CIP-009-6, and an associated implementation plan, on November 13, 2014. While these Reliability Standards are not being presented again for ballot or Board adoption, they are included herein for ease of reference and to provide a single implementation plan that contains all of the Reliability Standards adopted as part of Project 2014-02 CIP Version 5 Revisions.

Requested Board Withdrawals

NERC is requesting that the Board withdraw the following CIP Reliability Standards adopted by the Board of Trustees on November 13, 2014 and replace them with the revised versions of these CIP Reliability Standards presented to the Board on February 12, 2015:

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel & Training
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements**

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5.1 — Cyber Security — Personnel & Training
- CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

** The NERC Board of Trustees approved the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1 on November 13, 2014. While these Reliability Standards are not being presented again for retirement, they are included herein for ease of reference and to provide a single implementation plan that contains all of the requested Board actions as part of Project 2014-02 CIP Version 5 Revisions.

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples 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.
Transient Cyber Asset	A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is 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, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Low Impact BES Cyber System Electronic Access Point (LEAP)	A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Low Impact External Routable Connectivity (LERC)	Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), the additional time for compliance with that section is specified below. The compliance date for those particular sections represents the date that entities must begin to comply with that particular section of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-003-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R1, Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Requirement R2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 1 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 2

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 2 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 3

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 3 until the later of September 1, 2018 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

Compliance Date for CIP-003-6, Attachment 1, Section 4

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, Section 4 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. <u>CIP-004-6 — Cyber Security — Personnel & Training</u>

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable

governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security of BES Cyber Systems[1]

   Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-006-6, Requirement R1, Part 1.10

   For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 — Cyber Security — Systems Security Management

   Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the

[1] The NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with high and medium impact BES Cyber Systems until nine calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems[2]

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

[2] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.

Compliance Date for CIP-010-2, Requirement R4

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

   Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

   The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the compliance date for Reliability Standard CIP-010-2, Requirement R4, as applicable in the relevant jurisdiction.

   The new and modified NERC Glossary Terms Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity shall become effective on the compliance date for Reliability Standard CIP-003-6, Requirement R2, as applicable in the relevant jurisdiction.

9. Standards for Retirement[3]

   CIP-003-5 shall retire at midnight of the day immediately prior to the effective date of CIP-003-6 in the particular jurisdiction in which the new standard is becoming effective.

   CIP-004-5.1 shall retire at midnight of the day immediately prior to the effective date of CIP-004-6 in the particular jurisdiction in which the new standard is becoming effective.

[3] As noted above, the NERC Board retired these Reliability Standards in November 2014. Therefore, they are not being presented again for retirement but are included in this implementation plan for ease of reference.

CIP-006-5 shall retire at midnight of the day immediately prior to the effective date of CIP-006-6 in the particular jurisdiction in which the new standard is becoming effective.[4]

CIP-007-5 shall retire at midnight of the day immediately prior to the effective date of CIP-007-6 in the particular jurisdiction in which the new standard is becoming effective.

CIP-009-5 shall retire at midnight of the day immediately prior to the effective date of CIP-009-6 in the particular jurisdiction in which the new standard is becoming effective.[5]

CIP-010-1 shall retire at midnight of the day immediately prior to the effective date of CIP-010-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-011-1 shall retire at midnight of the day immediately prior to the effective date of CIP-011-2 in the particular jurisdiction in which the new standard is becoming effective.

10. Standards for Withdrawal

The withdrawal of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that were adopted by the Board in November 2014 shall become effective immediately upon Board adoption of the replacement Reliability Standards.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[6] (Version 5 Plan) remain the same:

[4] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.
[5] As noted above, the NERC Board adopted this standard and its implementation plan in November 2014. Therefore, it is not being presented again for ballot or for Board adoption but is included in this implementation plan for ease of reference.
[6] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

Unplanned Changes Resulting in Low Impact Categorization

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.