Implementation Plan

Project 2014-02 CIP Version 5 Revisions

September 3, 2014

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- 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
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-006-5 — Cyber Security — Physical Security
- 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
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

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	Media, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable Media are not Cyber Assets. 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, directly connected (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. 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 allows Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System.
Low Impact External Routable Connectivity (LERC)	Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (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 element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. <u>CIP-003-6 — Cyber Security — Security Management Controls</u>

   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, element 1

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 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, element 2

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

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

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Attachment 1, element 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, element 4

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

2. CIP-004-6 — Cyber Security — Personnel and Training

   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

   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 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 the elements of 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

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

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.

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 same compliance date as when Reliability Standard CIP-010-2, Requirement R4 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 same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that 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 same compliance date as when Reliability Standard CIP-003-6, Requirement R2 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 same compliance date as when Reliability Standard CIP-003-6, Requirement R2 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

9. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

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[1] (Version 5 Plan) remain the same:

- *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.

[1] 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