NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

~~September 3, 2014~~October 28, 2014

Requested Approvals

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

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5.1 — Cyber Security — Personnel ~~and~~& 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

This Implementation Plan is a combination of the effective dates for CIP-006-6 and CIP-009-6 from the initial ballot and the effective dates for the version X standards from the additional ballot. This Implementation Plan does not apply to standards revised to address the "Low Impact" and "Transient Device" directives from FERC Order No. 791. Those revisions require additional development and will be addressed in future versions of the standards with an associated Implementation Plan. ~~The standard version numbers currently include an (X) to indicate the version numbering will be updated. CIP-003-6 and CIP-010-2 for addressing the low impact assets and transient devices directives respectively were substantively revised and are posted concurrent with the IAC posting package. Depending on the ballot results of CIP-003-6 and CIP-010-2, NERC will assign the appropriate version number prior to NERC Board of Trustees adoption. The version X implementation plan is posted in a clean version although it draws upon the implementation plan from the previous posting and only includes language for those standards balloted as version X.~~

- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

None

~~**General Considerations**~~

~~The results of the initial CIP V5 Revisions ballot showed industry support for the new communication networks requirements and the removal of the identify, assess, and correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015.~~

~~The CIP-003-6 and CIP-010-2 revisions proposed to address the low impact and transient devices directives did not pass initial ballot. As a prudent approach and in order to meet the FERC filing deadline of February 3, 2015 for the two directives, the SDT would like to ballot the IAC revisions on their own without the low impact and transient devices revisions. Assuming the IAC revisions pass the second ballot, these standards can proceed to final ballot along with the communication networks revisions.~~

~~The SDT emphasizes that this is NOT an indication that it plans to separate the revision work. Strong progress continues on the low impact and transient devices revisions, and the SDT still hears support from stakeholders to complete all four directive areas of FERC Order No. 791 revisions at the same time. The request for a separate ballot is a practical measure to avoid potential complications with meeting FERC's directive deadlines that, if we were to wait until after the second ballot, time may not allow us to address.~~

~~The SDT plans to post a single ballot for the standards that need stakeholder approval for the IAC language removal. These proposed standards will be version X for the ballot. The version X ballot will be posted along with the other revision proposals designated with the appropriate version number. This allows for the simultaneous revision of the standards to address the directive issue areas and when both the version X and the numbered version standards pass ballot, the revisions can be combined into the appropriate numbered standard version.~~

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 with that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

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

   Reliability Standard CIP-003-~~X~~ 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-~~X~~6, Requirement R2

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

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

   Reliability Standard CIP-004-~~X~~ 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

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.

~~3.~~4. CIP-007-~~X~~6 —Cyber Security — Systems Security Management

Reliability Standard CIP-007-~~X~~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-~~X~~6, Requirement R1, Part 1.2

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-~~X~~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-~~X~~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 months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

~~4.~~6. CIP-010-~~X~~ 2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

Reliability Standard CIP-010-~~X~~ 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.

~~5.~~7. CIP-011-~~X~~ 2 — Cyber Security — Information Protection

Reliability Standard CIP-011-~~X~~ 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.

~~6.~~8. 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.~~

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.

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.

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.

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.

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