NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan ~~For~~for Version 5 CIP Cyber Security Standards

~~November 7, 2011~~

April 10, 2012

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* ~~Used~~used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards[1]," "[2] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security —-BES Cyber System ~~Identification~~Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
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

"Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, -and retirements of terms to the *Glossary of Terms ~~Used~~used in NERC Reliability Standards*.

These standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

---

[1] ~~Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1 in addition to CIP-002-5 through CIP-009-5 because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.~~

[2] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Compliance with Standards

Once these standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards become effective, the ~~Responsible Entities~~responsible entities identified in the Applicability ~~section~~Section of the standard must comply with the requirements. ~~These Responsible Entities include:~~

~~• Reliability Coordinator~~
~~• Balancing Authority~~
~~• Interchange Authority~~
~~• Transmission Owner~~
~~• Transmission Operator~~
~~• Generator Owner~~
~~• Generator Operator~~
~~• Load Serving Entity~~
~~• Distribution Provider~~
~~• NERC~~
~~• Regional Entity~~

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible ~~Entities~~entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards~~ as follows:

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5 R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[3]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[3] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement; such as, but not limited to, ". . . once each calendar year . . ." and responsible entities shall comply initially with those periodic requirements, as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5 R2
   - CIP-003-5 R4
2. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Secuirty Standards for the following requirements:
   - CIP-007-5 R4 Part 4.5
3. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Secuirty Standards for the following requirements:
   - CIP-007-5 R3 Part 3.3
   - CIP-010-1 R2 Part 2.1
4. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R6, Part 6.5
5. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R3, Part 3.2
   - CIP-004-5 R6, Parts 6.6 and 6.7
   - CIP-006-5 R3, Part 3.1
   - CIP-008-5 R2, Part 2.1
   - CIP-008-5 R3, Part 3.1
   - CIP-009-5 R2, Parts 2.1 and 2.2
   - CIP-009-5 R3, Part 3.1
   - CIP-010-5 R3, Parts 3.1 and 3.2
   - CIP-011-5 R1, Part 1.3

6. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5 R5 Part 5.2.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5 R4, Part 4.1.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System, as described in CIP-002-5, R1.1, which were planned and implemented by the ~~Responsible Entity~~responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in ~~Compliance~~compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5, R1.1, which were not planned by the ~~Responsible Entity.~~responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1~~. Then~~, 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, ~~or load patterns shift resulting in corresponding transmission flow changes through that transmission substation,~~ and that unchanged BES Cyber System may become a ~~Medium Impact~~ medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria~~. The actions that cause the change in power flows would have been performed by a neighboring entity and would result in a change in impact level the of the affected BES Cyber System~~.

For *planned* changes resulting in a higher categorization, the ~~Responsible Entity~~responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.1

For *unplanned* changes resulting in a higher categorization, the ~~Responsible Entity~~responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.~~1~~4:

Scenario of Unplanned Changes ~~After the Effective Date~~	Compliance Implementation
New ~~High Impact~~high impact BES Cyber System	12 months
New ~~Medium Impact~~medium impact BES Cyber System	12 months
Newly categorized ~~High Impact~~high impact BES Cyber System from ~~Medium Impact~~medium impact BES Cyber System	12 months for ~~new~~ requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized ~~Medium Impact~~medium impact BES Cyber System	12 months
Responsible ~~Entity Identifies~~entity identifies first ~~Medium~~medium impact or ~~High Impact~~high impact BES Cyber System	~~Add 12~~24 months ~~from time above~~

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 ~~R2~~, R1.

The rationale for this is that the primary task following a disaster is the restoration of the power system~~,~~ and the ability to serve customer ~~load~~Load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full ~~implementation of the CIP~~ compliance ~~implementation program~~with the Version 5 CIP Cyber Security Standards, restoration could be hampered~~,~~ and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to ~~implement~~comply with the Version 5 CIP ~~compliance implementation program~~Cyber Security Standards at the restored ~~facilities~~Facilities, and be able to demonstrate full compliance in a ~~spot-check~~spotcheck or audit; or~~,~~ file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

The following security requirements in CIP-003 through CIP-011 apply to these Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Cyber Security Training	X	X	
CIP-004-5 R4	Personnel Risk Assessment Program	X	X	
CIP-004-5 R5	Personnel Risk Assessment	X	X	
CIP-004-5 R6	Access Management Program	X	X	
CIP-004-5 R7	Access Revocation	X	X	
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X