NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan For Version 5 CIP Cyber Security Standards

November 7, 2011

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms 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]," are covered by this Implementation Plan:
CIP–002–5 —Cyber Security — BES Cyber System Identification
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 in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards*.

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

Compliance with Standards

Once these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority

[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.

- 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 shall comply with 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 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the 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.[2]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

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.

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 with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

[2] 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.

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. 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, 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 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 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 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:

Scenario of Unplanned Changes	Compliance Implementation
New High Impact BES Cyber System	12 months
New Medium Impact BES Cyber System	12 months
Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System	12 months for new requirements
Newly categorized Medium Impact BES Cyber System	12 months
Responsible Entity Identifies first Medium or High Impact BES Cyber System	Add 12 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.

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. 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, restoration could be hampered, and reliability could be harmed.

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