NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version ~~2~~3 of Cyber Security Standards CIP-002-~~2~~3 through CIP-009-~~2~~3

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

~~Modified~~Applicable Standards

The following standards ~~have been modified~~are covered by this Implementation Plan:

CIP–002–~~2~~3 — Cyber Security — Critical Cyber Asset Identification
CIP–003–~~2~~3 — Cyber Security — Security Management Controls
CIP–004–~~2~~3 — Cyber Security — Personnel and Training
CIP–005–~~2~~3 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–~~2~~3 — Cyber Security — Physical Security
CIP–007–~~2~~3 — Cyber Security — Systems Security Management
CIP–008–~~2~~3 — Cyber Security — Incident Reporting and Response Planning
CIP–009–~~2~~3 — Cyber Security — Recovery Plans for Critical Cyber Assets

~~Red-line versions of the above~~These standards are posted for ballot by NERC together with this Implementation Plan. When these ~~modified~~ standards become effective, ~~the~~all prior versions of these standards ~~and their Implementation Plan~~ are retired.

Compliance with Standards

Once these standards become effective, the ~~responsible entities~~Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

- NERC
- Regional Entity

~~Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.~~

Proposed Effective Date

~~The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).~~

~~For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.~~

The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 3 of the NERC Cyber Security Standards CIP-002-3 to CIP-009-3.

Prior Version Implementation Plan Retirement

By December 31, 2009, CIP Version 1's Table 1, 2, and 3 Registered Entities that registered prior to December 31, 2007 will have reached the "Compliant" milestone for all CIP Version 1 Requirements. Timetables for reaching the "Auditably Compliant" milestone will still be in effect for these Entities going forward until said timetables expire. As such, when Table 3 Registered Entities reach the Auditably Compliant milestone on December 31, 2010, the Version 1 Implementation Plan is in practice retired. Table 4 of the CIP Version 1 Implementation Plan is applicable only for newly Registered Entities, and compliance milestones for newly Registered Entities is included in CIP Version 2's Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities effective on April 1, 2010. CIP Version 3 milestones, are effective after FERC approval.