NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

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.

Applicable Standards

The following standards are covered by this Implementation Plan:

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

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these 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
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date

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.

Version 1 Implementation Plan Retirement

The Version 1 Implementation Plan will be retired once all Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state.

Version 2 Implementation Plan Retirement

The Version 2 Implementation Plan will be retired on April 1, 2010 or on a Version 1 legacy date for compliance that goes beyond April 1, 2010, whichever is later.