Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

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

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

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 for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard, or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4; (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage; or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

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

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. 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 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.