NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Implementation Plan for Cyber Security Standards
CIP-002-1 through CIP-009-1

The intent of the proposed NERC cyber security standards is to ensure that all entities responsible for the reliability of the bulk electric systems in North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems.

This implementation plan is based on the following assumptions:

- Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than November 1, 2005.
- Responsible Entities have registered.
- Cyber Security Standards CIP-002-1 through CIP-009-1 become effective November 1, 2005.

To provide time for Responsible Entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin in 2006. The table below lists specific periods by which applicable entities must be Auditably Compliant (defined below) with each requirement.

Implementation Schedule

The following tables identify when Responsible Entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement, or must Begin Work (BW) to become compliant with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. Substantially Compliant means an entity has begun to implement its plan to become compliant with a requirement, but is not yet Auditably Compliant. Begin Work means a responsible entity has developed a plan to address the requirements of a standard.

Table 1 defines the implementation schedule for Balancing Authorities (BA), Transmission Operators (TOP) that were required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200), and Reliability Coordinators (RC). Table 2 defines the implementation schedule for Transmission Providers (TP), those Transmission Operators (TOP) and Balancing Authorities that were not required to self-certify compliance to UA 1200, NERC, and the Regional Reliability Organizations.

Table 3 defines the implementation schedule for Interchange Authorities (IA), Transmission Owners (TO), Generator Owners (GO), Generator Operators (GOP) and Load Serving Entities (LSE). Because Functional Model registration does not include all Functional Model entities, this schedule is a time-based offset. This means that the implementation schedule begins upon an entity's registration (or certification) to a Functional Model function, as the Functional Model continues to be implemented.

Table 1
Compliance Schedule for Standards CIP-002-1 through CIP-009-1
Balancing Authorities and Transmission Operators Required to Self-certify to
UA Standard 1200, and Reliability Coordinators

	2nd Qtr 2006		2nd Qtr 2007		2nd Qtr 2008		2nd Qtr 2009	
Requirement	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
Standard CIP-002-1 — Critical Cyber Assets								
R1	SC	BW	AC	SC	AC	SC	AC	AC
R2	SC	BW	AC	SC	AC	SC	AC	AC
R3	SC	BW	AC	SC	AC	SC	AC	AC
Standard CIP-003-1 — Security Management Controls								
R1	SC	BW	AC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC	AC	AC
R3	SC	BW	SC	SC	AC	AC	AC	AC
R4	SC	BW	SC	SC	AC	AC	AC	AC
R5	SC	BW	SC	SC	AC	AC	AC	AC
R6	SC	BW	AC	SC	AC	AC	AC	AC
Standard CIP-004-1 — Personnel & Training								
R1	SC	BW	AC	SC	AC	AC	AC	AC
R2	SC	BW	AC	SC	AC	AC	AC	AC
R3	SC	BW	SC	SC	AC	SC	AC	AC
R4	SC	BW	AC	SC	AC	AC	AC	AC
Standard CIP-005-1 — Electronic Security								
R1	SC	BW	AC	SC	AC	SC	AC	AC
R2	SC	BW	AC	SC	AC	SC	AC	AC
R3	SC	BW	AC	SC	AC	SC	AC	AC
R4	SC	BW	AC	SC	AC	SC	AC	AC
R5	SC	BW	AC	SC	AC	SC	AC	AC
Standard CIP-006-1 — Physical Security								
R1	SC	BW	AC	SC	AC	SC	AC	AC

	2nd Qtr 2006		2nd Qtr 2007		2nd Qtr 2008		2nd Qtr 2009	
Requirement	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
R2	SC	BW	AC	SC	AC	SC	AC	AC
R3	SC	BW	AC	SC	AC	SC	AC	AC
R4	SC	BW	AC	SC	AC	SC	AC	AC
R5	SC	BW	AC	SC	AC	SC	AC	AC
R6	SC	BW	AC	SC	AC	SC	AC	AC
R7	SC	BW	AC	SC	AC	SC	AC	AC
Standard CIP-007-1 — Systems Security Management								
R1	SC	BW	AC	SC	AC	SC	AC	AC
R2	SC	BW	AC	SC	AC	SC	AC	AC
R3	SC	BW	AC	SC	AC	SC	AC	AC
R4	SC	BW	AC	SC	AC	SC	AC	AC
R5	SC	BW	AC	SC	AC	SC	AC	AC
R6	SC	BW	AC	SC	AC	SC	AC	AC
R7	SC	BW	AC	SC	AC	SC	AC	AC
R8	BW	BW	AC	SC	AC	SC	AC	AC
R9	BW	BW	SC	SC	AC	SC	AC	AC
R10	SC	BW	SC	SC	AC	SC	AC	AC
Standard CIP-008-1 — Incident Reporting and Response Planning								
R1	SC	BW	AC	AC	AC	AC	AC	AC
R2	SC	BW	AC	AC	AC	AC	AC	AC
Standard CIP-009-1 — Recovery Plans								
R1	SC	BW	AC	AC	AC	AC	AC	AC
R2	SC	BW	AC	SC	AC	AC	AC	AC
R3	SC	BW	AC	AC	AC	AC	AC	AC
R4	SC	BW	AC	AC	AC	AC	AC	AC
R5	SC	BW	AC	AC	AC	AC	AC	AC

Table 2
Compliance Schedule for Standards CIP-002-1 through CIP-009-1
Transmission Providers, those Balancing Authorities and Transmission Operators Not Required to Self-certify to UA Standard 1200, NERC, and Regional Reliability Organizations.

	2nd Qtr 2006	2nd Qtr 2007	2nd Qtr 2008	Dec. 31, 2009 & Beyond
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-002-1 — Critical Cyber Assets				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
Standard CIP-003-1 — Security Management Controls				
R1	BW	SC	AC	AC
R2	SC	AC	AC	AC
R3	BW	SC	AC	AC
R4	BW	SC	AC	AC
R5	BW	SC	AC	AC
R6	BW	SC	AC	AC
Standard CIP-004-1 — Personnel & Training				
R1	BW	SC	AC	AC
R2	BW	SC	AC	AC
R3	BW	SC	SC	AC
R4	BW	SC	AC	AC
Standard CIP-005-1 — Electronic Security				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
Standard CIP-006-1 — Physical Security				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC

	2nd Qtr 2006	2nd Qtr 2007	2nd Qtr 2008	Dec. 31, 2009 & Beyond
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
R6	BW	SC	SC	AC
R7	BW	SC	SC	AC
Standard CIP-007-1 — Systems Security Management				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
R6	BW	SC	SC	AC
R7	BW	SC	SC	AC
R8	BW	SC	SC	AC
R9	BW	SC	SC	AC
R10	BW	SC	SC	AC
Standard CIP-008-1 — Incident Reporting and Response Planning				
R1	BW	AC	AC	AC
R2	BW	AC	AC	AC
Standard CIP-009-1 — Recovery Plans				
R1	BW	AC	AC	AC
R2	BW	SC	AC	AC
R3	BW	AC	AC	AC
R4	BW	AC	AC	AC
R5	BW	AC	AC	AC

Table 3
Compliance Schedule for Standards CIP-002-1 through CIP-009-1
Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators, and Load-Serving Entities

	Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-002-1 — Critical Cyber Assets				
R1	BW	SC	AC	AC
R2	BW	SC	AC	AC
R3	BW	SC	AC	AC
Standard CIP-003-1 — Security Management Controls				
R1	BW	SC	AC	AC
R2	SC	AC	AC	AC
R3	BW	SC	AC	AC
R4	BW	SC	AC	AC
R5	BW	SC	AC	AC
R6	BW	SC	AC	AC
Standard CIP-004-1 — Personnel & Training				
R1	BW	SC	AC	AC
R2	BW	SC	AC	AC
R3	BW	SC	SC	AC
R4	BW	SC	AC	AC
Standard CIP-005-1 — Electronic Security				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
Standard CIP-006-1 — Physical Security				
R1	BW	SC	SC	AC

	Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
R6	BW	SC	SC	AC
R7	BW	SC	SC	AC
Standard CIP-007-1 — Systems Security Management				
R1	BW	SC	SC	AC
R2	BW	SC	SC	AC
R3	BW	SC	SC	AC
R4	BW	SC	SC	AC
R5	BW	SC	SC	AC
R6	BW	SC	SC	AC
R7	BW	SC	SC	AC
R8	BW	SC	SC	AC
R9	BW	SC	SC	AC
R10	BW	SC	SC	AC
Standard CIP-008-1 — Incident Reporting and Response Planning				
R1	BW	SC	AC	AC
R2	BW	SC	AC	AC
Standard CIP-009-1 — Recovery Plans				
R1	BW	AC	AC	AC
R2	BW	SC	AC	AC
R3	BW	AC	AC	AC
R4	BW	AC	AC	AC
R5	BW	AC	AC	AC