NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

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

The intent of the proposed 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 May 2, 2006.
- Responsible Entities have registered.
- Cyber Security Standards CIP-002-1 through CIP-009-1 become effective June 1, 2006.

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 2007. The table below lists specific periods by which applicable Responsible Entities must be Auditably Compliant (defined below) with each requirement.

Implementation Schedule

The following tables identify when Responsible Entities must Begin Work (BW) to become compliant with a requirement, Substantially Compliant (SC) with a requirement, Compliant (C) with a requirement, and Auditably Compliant (AC) with a requirement. Begin Work means a Responsible Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements. Substantially Compliant means an entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant. Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records." Auditably Compliant means the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records." Per the standards, each subsequent compliance-monitoring period will require the previous full calendar year of such material.

The implementation plan is broken into four tables as described below. The tables specify a compliance schedule for NERC Functional Model "entities," referred to as Responsible Entities in CIP-002 through CIP-009 standards. For organizations that are multiple Functional Model entities, each such Functional Model entity is required to demonstrate progress towards compliance according to the applicable table.

For instance, Table 1 applies to the Energy Control Center (Balancing Authority and Transmission Operator who were required to self-certify under Urgent Action Standard 1200) while the same organization's Generating Plant function (Generation Owners), would use Table 3. Likewise, this same organization's Transmission Provider function would use Table 2.

Table 1 defines the implementation schedule for Balancing Authorities (BA), Transmission Operators (TOP), and Reliability Coordinators (RC) that were required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200).

Table 2 defines the implementation schedule for Transmission Service Providers (TSP), 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 Responsible Entities required to register during 2006.

Table 4 defines the implementation schedule for Responsible Entities registering to a Functional Model function in 2007 and thereafter.

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

	End of 2nd Qtr 2007		End of 2nd Qtr 2008		End of 2nd Qtr 2009		End of 2nd Qtr 2010	
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	C	SC	AC	C	AC	AC
R2	SC	BW	C	SC	AC	C	AC	AC
R3	SC	BW	C	SC	AC	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-003-1 — Security Management Controls								
R1	SC	BW	C	SC	AC	AC	AC	AC
R2	SC	SC	C	C	AC	AC	AC	AC
R3	SC	BW	C	SC	AC	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
R5	BW	BW	SC	SC	C	C	AC	AC

Table 1 (cont.)

	End of 2nd Qtr 2007		End of 2nd Qtr 2008		End of 2nd Qtr 2009		End of 2nd Qtr 2010	
Requirement	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
R6	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-004-1 — Personnel & Training								
R1	BW	BW	SC	SC	C	C	AC	AC
R2	SC	BW	C	SC	AC	C	AC	AC
R3	SC	BW	C	SC	AC	C	AC	AC
R4	SC	BW	C	SC	AC	C	AC	AC
Standard CIP-005-1 — Electronic Security								
R1	BW	BW	SC	SC	C	C	AC	AC
R2	BW	BW	SC	SC	C	C	AC	AC
R3	BW	BW	SC	SC	C	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
R5	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-006-1 — Physical Security								
R1	BW	BW	SC	SC	C	C	AC	AC
R2	BW	BW	SC	SC	C	C	AC	AC
R3	BW	BW	SC	SC	C	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
R5	BW	BW	SC	SC	C	C	AC	AC
R6	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-007-1 — Systems Security Management								
R1	SC	BW	C	SC	AC	C	AC	AC
R2	BW	BW	SC	SC	C	C	AC	AC
R3	BW	BW	SC	SC	C	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
R5	BW	BW	SC	SC	C	C	AC	AC

Table 1 (cont.)

	End of 2nd Qtr 2007		End of 2nd Qtr 2008		End of 2nd Qtr 2009		End of 2nd Qtr 2010	
Requirement	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities	System Control Center	Other Facilities
R6	BW	BW	SC	SC	C	C	AC	AC
R7	BW	BW	SC	SC	C	C	AC	AC
R8	BW	BW	SC	SC	C	C	AC	AC
R9	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-008-1 — Incident Reporting and Response Planning								
R1	SC	BW	C	SC	AC	C	AC	AC
R2	BW	BW	SC	SC	C	C	AC	AC
Standard CIP-009-1 — Recovery Plans								
R1	SC	BW	C	SC	AC	C	AC	AC
R2	SC	BW	C	SC	AC	C	AC	AC
R3	BW	BW	SC	SC	C	C	AC	AC
R4	BW	BW	SC	SC	C	C	AC	AC
R5	BW	BW	SC	SC	C	C	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.

	End of 2nd Qtr 2007	End of 2nd Qtr 2008	End of 2nd Qtr 2009	End of 2nd Qtr 2010
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-002-1 — Critical Cyber Assets				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
Standard CIP-003-1 — Security Management Controls				
R1	BW	SC	C	AC
R2	SC	C	AC	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
Standard CIP-004-1 — Personnel & Training				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
Standard CIP-005-1 — Electronic Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC

Table 2 (cont.)

Standard CIP-006-1 — Physical Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
	Standard CIP-007-1 — Systems Security Management			
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
R7	BW	SC	C	AC
R8	BW	SC	C	AC
R9	BW	SC	C	AC
Standard CIP-008-1 — Incident Reporting and Response Planning				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
Standard CIP-009-1 — Recovery Plans				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	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

	December 31, 2006	December 31, 2008	December 31, 2009	December 31, 2010
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-002-1 — Critical Cyber Assets				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
Standard CIP-003-1 — Security Management Controls				
R1	BW	SC	C	AC
R2	SC	C	AC	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
Standard CIP-004-1 — Personnel & Training				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
Standard CIP-005-1 — Electronic Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC

Table 3 (cont.)

	December 31, 2006	December 31, 2008	December 31, 2009	December 31, 2010
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-006-1 — Physical Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
Standard CIP-007-1 — Systems Security Management				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
R7	BW	SC	C	AC
R8	BW	SC	C	AC
R9	BW	SC	C	AC
Standard CIP-008-1 — Incident Reporting and Response Planning				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
Standard CIP-009-1 — Recovery Plans				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC

Table 3 (cont.)

	December 31, 2006	December 31, 2008	December 31, 2009	December 31, 2010
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
R5	BW	SC	C	AC

Table 4
Compliance Schedule for Standards CIP-002-1 through CIP-009-1
For Entities Registering in 2007 and Thereafter.

	Upon 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	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
Standard CIP-003-1 — Security Management Controls				
R1	BW	SC	C	AC
R2	SC	C	AC	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
Standard CIP-004-1 — Personnel & Training				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC

Table 4 (cont.)

	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-005-1 — Electronic Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
Standard CIP-006-1 — Physical Security				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
Standard CIP-007-1 — Systems Security Management				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC
R6	BW	SC	C	AC
R7	BW	SC	C	AC
R8	BW	SC	C	AC
R9	BW	SC	C	AC

Table 4 (cont.)

	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
Standard CIP-008-1 — Incident Reporting and Response Planning				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
Standard CIP-009-1 — Recovery Plans				
R1	BW	SC	C	AC
R2	BW	SC	C	AC
R3	BW	SC	C	AC
R4	BW	SC	C	AC
R5	BW	SC	C	AC