NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Guidance for Enforcement of CIP Standards

In Order No. 706, the Federal Energy Regulatory Commission approved the CIP-002 through CIP-009 Reliability Standards and NERC's proposed implementation plan. This document provides guidance and makes clear two issues regarding implementation and enforcement of the CIP standards.

I. Applicability of Penalties and Sanctions for Standards CIP-002 through CIP-009

NERC received several inquiries regarding whether penalties and sanctions apply to Registered Entities at the "Compliant" stage or only apply at the "Auditably Compliant" stage. NERC consulted with FERC staff and was advised that Order No. 706 provides that sanctions and penalties apply at the "Compliant" stage. In particular, FERC staff stated that the reference in paragraph 97 of Order 706 to "achieving full compliance" means an entity becoming "Compliant," as defined in the approved implementation plan. FERC staff recognized that for requirements that direct periodic reviews or depend upon accumulation of information over time, the requirements would not be evaluated until the end of the applicable period. FERC staff stated their advice is not binding on the Commission.

Therefore, on July 1, 2008, thirteen Requirements embodied in CIP-002 through CIP-009 become enforceable at the "Compliant" stage for responsible entities covered by Table 1 of the implementation plan. These Requirements include the following:

CIP-002-1: R.1 – R.3
CIP-003-1: R.1 – R.3
CIP-004-1: R.2 – R.4
CIP-007-1: R.1
CIP-008-1: R.1
CIP-009-1: R.1 – R.2.

In addition, on July 1, 2008 CIP-003, R2 becomes enforceable at the "Compliant" stage for responsible entities covered by Table 2 of the implementation plan.

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

To achieve a consistent approach to the implementation and enforcement of CIP-002 through CIP-009, NERC provides the following additional information:

Audits begin July 1, 2009
NERC and the Regional Entities will not conduct Compliance Audits in 2008 with respect to the enforceable Requirements in CIP-002 through CIP-009 noted above; rather, Compliance Audits for these Requirements will begin July 1, 2009.

Self-certification begins July 1, 2008
As of July 1, 2008, the Requirements noted above **will be** subject to self certifications, self reporting, investigations and other monitoring mechanisms, other than audits, outlined in the NERC Compliance Monitoring Enforcement Program (CMEP), set forth in Appendix 4C of the NERC *Rules of Procedure*.

Self Reporting and submittal of Mitigation Plans
For Registered Entities that self report possible violations of the Requirements noted above prior to July 1, 2008, the Regional Entities will have discretion not to apply penalties and sanctions in the event that appropriate mitigation plans are in place and implemented in accordance with terms and conditions approved by the applicable Regional Entity and NERC.

Enforcement Considerations for Self Reports and Self Certifications
On July 1, 2008, the Regional Entities have the responsibility to enforce the approved CIP 002-CIP 009 standards in the US in accordance with the implementation plan. For the remainder of 2008, Regional Entities will apply their discretion with the application of any financial penalties for confirmed violations. Further, users, owners, and operators self reporting non-compliance with the requirements and submitting and implementing appropriate mitigation plans will alleviate the prospect of financial penalties during the period of the mitigation plan.

II. Explanation of the Tables in the CIP 002 – CIP 009 Implementation Plan

NERC provides the following explanation and clarification for Tables 1 through 4 of the approved CIP Implementation Plan.

Table 1
Table 1 covers only those Balancing Authorities and Transmission Operators that self-certified under Urgent Action 1200 and Reliability Coordinators. Table 1 is not based on the date Registered Entities were included on the NERC Compliance Registry. There is no change with respect to implementation Table 1. Registered Entities covered by Table 1 must be compliant by July 1, 2008 for the thirteen requirements identified above that become enforceable at the “Compliant” stage.

Tables 2, 3, and 4
During the past several weeks NERC has examined the NERC Compliance Registry process and how registration applies to the CIP 002 – CIP 009 Implementation Plan for Tables 2, 3 and 4. The registration of responsible entities that took place prior to 2007 was undertaken under the auspices of the voluntary compliance regime and was not binding on any future legislation or rules subsequently passed by NERC or FERC. Registration of entities for the mandatory reliability standards began in March 2007, after NERC was certified as the ERO in the United States and the Commission approved NERC's registration criteria. Registered Entities were notified by NERC of the date they were included on the NERC Compliance Registry subjecting the entity to mandatory reliability standards in the United States once an applicable standard was approved. The analysis determined that July 1, 2008 is the first date that an entity could be subject to penalties at the "Compliant" stage. Based on this information, NERC views the Implementation Plan for Registered Entities under Table 2, 3 and 4 as follows:

Table 2
Table 2 is the Compliance Schedule for Standards CIP-002-1 through CIP-009-1 for (i) all Transmission Service Providers, (ii) those Balancing Authorities and Transmission Operators not required to self-certify to Urgent Action Standard 1200, (iii) NERC, and (iv) Regional Entities.

Table 2 example:

A Transmission Service Provider has a Compliance Registry date of May 29, 2007. Based on table descriptions, the entity would be subject to Table 4 because they have a registration date in 2007. With a registration date of May 29, 2007, the entity would have to be Compliant with CIP 003, Requirement 2 and Substantially Compliant with all other requirements on May 29, 2008. In this example Table 4 would impose a slightly accelerated schedule to the July 1, 2008 date. Therefore, the entity is subject to Table 2, the least restrictive table for their registration.

Table 3
Table 3 is the Compliance Schedule for Standards CIP-002-1 through CIP-009-1 for Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators, and Load-Serving Entities. Table 3 will be utilized based on the NERC Compliance Registry date. As stated earlier, and similar to Table 1 methodology, no one is forced to comply before December 2009 (except for the December 2008 compliance deadline for CIP-003, Requirement 2) if you are in Table 3; no one should be accelerated by virtue of the fact they were registered in 2007.

Table 3 example:

A Generator Owner/Generator Operator has a Compliance Registry date of May 31, 2007. Based on table descriptions, the entity would be subject to Table 4 because they

have a registration date in 2007. With a registration date of May 31, 2007, the entity would have to be Compliant with CIP 003, Requirement 2 and Substantially Compliant with all other requirements on May 31, 2008. In this example, Table 4 would impose a seven month accelerated schedule to the December 31, 2008 date of Table 3. Therefore, the entity is subject to Table 3, the least restrictive table for their registration.

Table 4

Table 4 is the Compliance Schedule for Standards CIP-002-1 through CIP-009-1 for entities registered in 2007 and thereafter that are not covered in Table 1, Table 2 and Table 3 as outlined above. Table 4 was intended to provide an ongoing compliance implementation schedule for entities registered after the initial effort to register owners, operators, and users of the bulk power system. It was not intended to accelerate the compliance responsibilities of the entities covered by Tables 1, 2, and 3.

All Tables

Registered Entities with multiple functions could be covered by different tables for compliance for their different functions. Example: A Registered Entity self-certified to Urgent Action 1200 as a Balancing Authority and is also registered as a Transmission Service Provider and Generator Owner with a Compliance Registry date of May 31, 2007. This Registered Entity would be assigned to Table 1 for its Balancing Authority function, Table 2 for its Transmission Service Provider function, and Table 3 for its Generator Owner function.

In conclusion, all CIP Implementation Tables will be implemented but will not accelerate any compliance requirements for those entities registered in 2007.

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