

**ISO/RTO Council Comments on the
Implementation Plan
for Cyber Security Standards
CIP-002-1 through CIP-009-1**

2/16/05

<p>The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems.</p> <p>This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, 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 September 1, 2005. The NERC Functional Model is implemented in concert with the passage of the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005.</p> <p>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 starting in 2006.</p> <p>Implementation Schedule</p> <p>Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the</p>	<p>The following is the position of the ISO/RTO Council Members:</p> <p>Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006.</p> <ul style="list-style-type: none"> • NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort. • No budgeting can typically be done until the standards are confirmed and solidified. • Most budgets are confirmed four or five months prior to the fiscal target year. <p>Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little impact and should be acceptable in view of the development of this new and major standard.</p> <p>The implementation plan should recognize typical corporate fiscal planning processes.</p> <p>Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis.</p>
--	---

applicable functional entities within their respective Regions. Regions may ask other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary.

All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the “Responsible Entity”.

The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor.

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of 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, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC

Recommendation: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.

Board of Trustees no later than September 1, 2005.

The NERC Functional Model is implemented in concert with the passage of the Version 0 standards.

Entities have registered to the NERC Functional Model.

Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 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 starting in 2006.

Implementation Schedule

Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary.

All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these

standards remains with the “Responsible Entity”.

The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) 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 the process to become compliant with a requirement, but is not yet Auditably Compliant.

The table has two sections for each standard. The first section defines the implementation schedule for Balancing Authorities (BA) and Reliability Coordinators (RC). The second section defines the implementation schedule for Interchange Authorities (IA), Transmission Providers (TP), Transmission Owners (TO), Transmission Operators (TOP), Generation Owners (GO), Generation Operators (GOP) and Load Serving Entities (LSE).

--	--

Compliance Schedule for Standards CIP-002-1 through CIP-009-1

	1st Qtr		1st Qtr 2007		2008 & Beyond	
Requi	Co ntr	Other Facilit	Contr ol	Other Facilitol	Contr ol	Other Facilities
Standard CIP-002-1 – Critical Cyber Assets BA & RC						
FAC	SC	AC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC	AC
Standard CIP-002-1 – Critical Cyber Assets IA, TP, TO, TOP, GO, GOP, LSE						
FSC	SC	AC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls						
FAC	SC	AC	AC	AC	AC	AC

FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls					
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
Standard CIP-004-1 – Personnel & Training BA & RC					
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
Requirement	Control	Other Facilities	Control	Other Facilities	Control	Other Facilities
R4	SC	SC	SC	SC	AC	AC
Standard CIP-004-1 – Personnel & Training						
IA TP TO TOP GO GOP LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	SC	SC	AC	AC
Standard CIP-005-1 – Electronic Security						
BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-005-1 – Electronic Security						
IA TP TO TOP GO GOP LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security						
BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security						
IA TP TO TOP GO GOP LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-007-1 – Systems Security Management						

NERC Cyber Security Standards – CIP-002-1 through CIP-009-1

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
COMM	Contr ol	Other Facilit	Contr ol	Other Facilit	Contr ol	Other Facilit
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
Standard CIP-009-1 – Recovery Plans IA, TP, TO, TOP, GO, GOP, LSE						
	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC