

---

# NERC 1200 and CIP-002 through CIP-009 Comparison

---

Original: May 11, 2005

Updated: January 30, 2006

By Nick Lauriat and Adam Lipson

<http://www.netsectech.com/>

**Version 3**

Prepared For:

ISO New England  
One Sullivan Road  
Holyoke, MA 01040

Prepared By:

Network & Security Technologies  
161 North Middletown Road  
Pearl River, NY 10965-2029



*Copyright ©2006, Network & Security Technologies, All Rights Reserved*

*This document was prepared by Network & Security Technologies, Inc. It may contain confidential or proprietary information. Any distribution or copying of the contents of this document, in whole or in part requires the express written permission of Network & Security Technologies, Inc.*

*All product or brand names are trademarks or registered trademarks of their respective owners.*

## Executive Summary

ISO New England and Network & Security Technologies, Inc. (N&ST) have compared the following two cyber security standards from North American Electric Reliability Council (NERC):

1. "Urgent Action Standard 1200 – Cyber Security" (NERC 1200), and
2. "CIP-002-1" through "CIP-009-1", Draft 4 (NERC CIP).

This document summarizes NERC's activities and describes the difference between these two standards. In an effort to maximize the usefulness of this document, N&ST has summarized the information into a table that identifies the requirements in NERC CIP, any relevant requirement from NERC 1200, and comments on the differences. This table is based on the current draft versions of the NERC CIP.

ISO New England originally hired N&ST to compile this comparison based on NERC CIP Draft 3. This document was submitted to NERC as part of ISO New England's comments on Draft 3. When Draft 4 was released, N&ST updated this document to reflect the changes in the NERC CIP standard.

This document is not focused on any one utility's compliance program; instead, it examines the basic differences between NERC 1200 and NERC CIP. N&ST understands that NERC CIP is in draft form, and that both the standards and the implementation plan may continue to change before they are finalized.

ISO New England invites other utilities to take advantage of this gap analysis. Every utility needs to understand how much effort might be required to meet the requirements identified in the standard by the dates in the initial Implementation Plan.

**Table of Contents**

Executive Summary ..... 2

Table of Contents ..... 3

Authors ..... 4

Network & Security Technologies, Inc. .... 4

ISO New England ..... 4

Background ..... 5

NERC CIP Table ..... 7

NERC CIP-002-1 – Critical Cyber Asset Identification ..... 8

NERC CIP-003-1 – Security Management Controls ..... 10

NERC CIP-004-1 – Personnel and Training ..... 13

NERC CIP-005-1 – Electronic Security Perimeter(s) ..... 16

NERC CIP-006-1 – Physical Security of Critical Cyber Assets ..... 21

NERC CIP-007-1 – Systems Security Management ..... 25

NERC CIP-008-1 – Incident Reporting and Response Planning ..... 31

NERC CIP-009-1 – Recovery Plans for Critical Cyber Assets ..... 33

Bibliography ..... 35

NERC 1200 ..... 35

NERC CIP Draft 4 ..... 35

NERC CIP Draft 3 ..... 35

NERC CIP Draft 2 ..... 36

Other Documents ..... 36

## Authors

### ***Network & Security Technologies, Inc.***

Nick Lauriat

161 North Middletown Road

Pearl River, NY 10965

**Mobile:** 781-572-1400

Adam Lipson

161 North Middletown Road

Pearl River, NY 10965

**Office:** 845-620-9500

**Mobile:** 914-552-3700

### ***ISO New England***

Chuck Noble

One Sullivan Road

Holyoke, MA 01040

**Office:** 413-540-4232

## Background

NERC's development of the permanent cyber security standard was initiated in July, 2003 when the NERC Standards Authorization Committee (SAC) approved Standard 1300 Standards Authorization Request (SAR) Draft 1. In December 2003, the SAC approved Draft 2 of the Standard 1300 SAR and in June, 2004 the SAC appoints a drafting team for Standard 1300. In September 2004, the Standard 1300 – Cyber Security first draft was released for public review and comment. After receiving numerous comments and suggestions, the Standard was revised and Draft 2 was released in January 2005. To comply with NERC's naming convention, Standard 1300 had been broken in to eight separate standards, now referred to as standards "CIP-002-1" through "CIP-009-1."

N&ST originally reviewed Draft 3 of the permanent cyber security standard for ISO New England. This version of this document addresses Draft 4 of NERC CIP, which is expected to be the final version submitted for balloting. Draft 4 will be balloted in the late winter and early spring, with final ratification by the NERC Board of Trustees in May of 2006. The concurrent Implementation Plan for the NERC CIP standards requires utilities who self-certified for NERC 1200 to be "Substantially Compliant"<sup>1</sup> or "Compliant"<sup>2</sup> by June 30, 2008 (see definitions from Implementation Plan for Cyber Security Standards below). Other utilities will have slightly more time to prepare for NERC CIP compliance.

The permanent cyber security standard is divided in to eight separate reliability standards:

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

---

<sup>1</sup> "Substantially Compliant" means the Responsible Entity "is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant."

<sup>2</sup> "Compliant" means the Responsible Entity "meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' logs,' and 'records.'"

These eight standards cover all of the same areas covered by the NERC Urgent Action Standard, but from a different point of view. Instead of organizations identifying their critical cyber assets directly, organizations must identify their critical assets and then extrapolate their critical cyber assets.

NERC's efforts have gone a long way to ensure the security of the United States bulk electric system. NERC's permanent standards will identify the minimum requirements to implement and maintain a cyber security program and to protect cyber assets critical to reliable bulk electric system operation. It is critical that standards are established to protect critical cyber assets to ensure the reliable operations.

## NERC CIP Table

In this section, N&ST analyzes the eight NERC CIP documents for differences that will likely cause a significant impact on many utilities. N&ST has included the requirement text from Draft 4 of the NERC CIP standards. While it is expected that this requirement text will change before the standard is ratified, the current version of the text can give the reader an impression of the content likely to be contained within each CIP standard. At the same time, N&ST chose not to include the text for the Measures section or the Compliance section; with ISO-NE's permission, N&ST focused exclusively on the requirements.

As in the example below, N&ST has indicated requirements that are new (or have substantially changed) by shading the relevant comments cell in light yellow.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-00x-1	Rx	Example Requirement Text	Relevant NERC 1200 Standard	Example Comments
CIP-00x-1	Rx	Example Requirement Text	No Reference Found	Example Comments

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-002-1 – Critical Cyber Asset Identification</b>				
CIP-002-1	R1	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No Reference Found	<p>NERC CIP-002 takes a different approach than NERC 1200 to identifying the boundaries of the cyber security standard. The new standard states that responsible entities must identify their Critical Assets using a “risk-based assessment methodology” (and R1 goes on to suggest a minimum set of Critical Assets to be considered in that methodology), use that methodology, and then determine their Critical Cyber Assets.</p> <p>Every Responsible Entity will need to quickly start a process to identify an appropriate risk-based assessment approach and the resulting Critical Assets. N&amp;ST believes that the risk-based assessment does not have to be complex, but it does have to include “procedures and evaluation criteria.”</p> <p>Every organization’s unique position in the grid means that every organization will have a unique list of Critical Assets. Responsible Entities will also likely need to work with their Regional Reliability Council and their Regional Transmission Organization on their list, since those organizations will be involved in compliance efforts.</p> <p>At a minimum, most organizations will have a control center and backup control center that will qualify as Critical Assets. The cyber assets that provide the data/information to drive the decisions made in the control room are critical cyber assets. Because of today’s complex control room environment, many systems are involved in supporting control room activities. Even if the control room is the only Critical Assets, it will likely lead to a substantial list of Critical Cyber Assets.</p> <p>Other organizations will have a long list of Critical Assets, ranging from generating stations to critical substations. All of the cyber assets (including both data acquisition and protection equipment) must be at least considered for inclusion on the critical cyber asset list.</p>
CIP-002-1	R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.		
CIP-002-1	R1.2	The risk-based assessment shall consider the following assets:		
CIP-002-1	R1.2.1	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.		
CIP-002-1	R1.2.2	Transmission substations that support the reliable operation of the Bulk Electric System.		
CIP-002-1	R1.2.3	Generation resources that support the reliable operation of the Bulk Electric System.		
CIP-002-1	R1.2.4	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.		
CIP-002-1	R1.2.5	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.		
CIP-002-1	R1.2.6	Special Protection Systems that support the reliable operation of the Bulk Electric System.		
CIP-002-1	R1.2.7	Any additional assets that support the reliable operation of the Bulk Electric System that the responsible Entity deems appropriate to include in its assessment.		
CIP-002-1	R2	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-002-1	R3	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	NERC 1202 – Critical Cyber Assets	<p>NERC 1202 – Critical Cyber Assets takes the approach that responsible entities “shall maintain a document identifying critical cyber assets.” Later guidance from NERC suggested that this only applied to cyber assets contained within the SCADA aggregation points – not remote devices in substations such as relays and RTUs. The new standard states that responsible entities must identify their Critical Assets, and then determine their Critical Cyber Assets – and are no longer limited to cyber assets contained within the SCADA aggregation points.</p> <p>There are some limits on these cyber assets, however, since the cyber asset has to be dial-up accessible or use a routable protocol (with an upstream connection) for communication. This means that remote equipment (RTUs and relays, for example) that use a serial SCADA protocol and do not have dial-up access are not Critical Cyber Assets.</p>
CIP-002-1	R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,		
CIP-002-1	R3.2	The Cyber Asset uses a routable protocol within a Control Center; or,		
CIP-002-1	R3.3	The Cyber Asset is dial-up accessible.		
CIP-002-1	R4	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)’s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	NERC 1201 – Cyber Security Policy	NERC 1201 requires: “The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity’s cyber security program.” While this is different than a senior manager reviewing and approving the list of Critical Assets and the list of Critical Cyber Assets, it will probably be done by the same person – causing no additional burden on the Responsible Entity.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-003-1 – Security Management Controls</b>				
CIP-003-1	R1	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management’s commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	NERC 1201 – Cyber Security Policy	NERC CIP-003 is a combination of requirements from several sections of NERC 1200. Primarily, the first requirement (for a security policy to be created and maintained) is directly from NERC 1201 – Cyber Security Policy. A NERC 1200 compliant Responsible Entity should have no trouble demonstrating compliance with this requirement.
CIP-003-1	R1.1	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.		
CIP-003-1	R1.2	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.		
CIP-003-1	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.		
CIP-003-1	R2	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009.	NERC 1201 – Cyber Security Policy	NERC 1201 states: “The responsible entity shall assign a member of senior management with responsibility for leading and managing the entity’s cyber security program.”  Because of the similarity of the requirements, Responsible Entities should have no trouble complying with the requirement.
CIP-003-1	R2.1	The senior manager shall be identified by name, title, business phone, business address, and date of designation.		
CIP-003-1	R2.2	Changes to the senior manager must be documented within thirty calendar days of the effective date.		
CIP-003-1	R2.3	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.		
CIP-003-1	R3	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	NERC 1201 – Cyber Security Policy	NERC 1201 states the person in charge of the Cyber Security program: “must authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption must be documented.”  Most Responsible Entities should have already created an exception process to fully comply with NERC 1201. The new standard now states that Responsible Entities must “include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.” This means the documentation for exceptions may have to be
CIP-003-1	R3.1	Exceptions to the Responsible Entity’s cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).		
CIP-003-1	R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-003-1	R3.3	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.		revised, but this is a reasonable goal for Responsible Entities.  If the senior manager is not already reviewing the exceptions on a regular basis, they must begin doing that to ensure compliance with NERC CIP.
CIP-003-1	R4	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	NERC 1210 – Information Protection	<p>NERC CIP-003 Requirements 4 and 5 comes from NERC 1210 – Information Protection, but the requirements are significantly more complex. NERC 1210 simply requires that Responsible Entities: "shall protect information associated with critical cyber assets and the policies and practices used to keep them secure."</p> <p>NERC CIP-003 Requirements 4 and 5 significantly extend NERC 1200 by requiring a formal program for categorizing critical information and a formal annual review of its adherence to the program. This is not required by NERC 1200, and may take some significant effort to implement properly, especially at large responsible entities that handle large amounts of critical information. NERC 1210 only requires reviewing the document annual – not the program itself or its adherence.</p> <p>One of the ways that Requirement 5 goes further than NERC 1210 is by requiring Responsible Entities to also document who is allowed to grant access. This will require Responsible Entities to improve their information protection programs to meet these new documentation requirements.</p>
CIP-003-1	R4.1	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.		
CIP-003-1	R4.2	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.		
CIP-003-1	R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
CIP-003-1	R5	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.		
CIP-003-1	R5.1	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.		
CIP-003-1	R5.1.1	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.		
CIP-003-1	R5.1.2	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.		
CIP-003-1	R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-003-1	R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.		
CIP-003-1	R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	NERC 1213 – Test Procedures	Requirement 6 discusses the need for change control procedures for changes to critical cyber assets. While this is a derivative of NERC 1213 – Test Procedures, it goes significantly further than the requirements in NERC 1213. NERC 1213 simply requires that critical cyber assets installed or modified comply with the NERC 1200 standard, and that all testing and acceptance be done in an isolated environment. The new Requirement 6 requires a very formal testing and change control program – something that may not have been created for NERC 1200 compliance.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-004-1 – Personnel and Training</b>				
CIP-004-1	R1	<p>Awareness — The Responsible Entity shall establish, maintain, and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:</p> <ul style="list-style-type: none"> <li>• Direct communications (e.g., emails, memos, computer based training, etc.);</li> <li>• Indirect communications (e.g., posters, intranet, brochures, etc.);</li> <li>• Management support (e.g., presentations, all-hands meetings, etc.).</li> </ul>	No Reference Found	Requirement 1 of CIP-004 is a slightly new twist on the training requirement – requiring a quarterly “awareness” program that goes above and beyond the annual training. This may require some extra effort by Responsible Entities to ensure NERC CIP compliance.
CIP-004-1	R2	<p>Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.</p>	<p>NERC 1207 – Personnel and NERC 1211 – Training</p>	<p>Requirement 2 (Training) is directly from 1211 – Training, and will not likely require a major revision of materials prepared for NERC 1200 compliance. This requirement is likely being addressed already by Responsible Entities who self-certified for compliance with NERC 1200.</p> <p>The training materials should be reviewed, however, to ensure that new aspects of NERC CIP are addressed adequately.</p>
CIP-004-1	R2.1	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.		
CIP-004-1	R2.2	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:		
CIP-004-1	R2.2.1	The proper use of Critical Cyber Assets;		
CIP-004-1	R.2.2.2	Physical and electronic access controls to Critical Cyber Assets;		
CIP-004-1	R2.2.3	The proper handling of Critical Cyber Asset information; and,		
CIP-004-1	R2.2.4	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.		
CIP-004-1	R2.3	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-004-1	R3	Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	NERC 1207 – Personnel	<p>NERC has wisely changed the very prescriptive language of 1207 (“background screening”) to the more reasonable “Personnel Risk Assessment” in CIP-004 Requirement 4. Responsible Entities will have to document how they screen prospective and current employees, and then keep records on which employees and contractors have been screened, and which employees and contractors have participated in training and awareness programs.</p> <p>The new requirement gives Responsible Entities the latitude to implement appropriate Personnel Risk Assessments without violating other standards. Developing an acceptable Personnel Risk Assessment may take Responsible Entities some time, however, since it will have to be done in close coordination with Legal and HR personnel – and may require investigating what type of background investigation is acceptable for a particular organization.</p> <p>It is important to note, however, that the FAQs state: “Employees, contractors, or service providers who have had a personnel risk assessment within the previous 7 years from the implementation date of the Standard do not need to be reassessed until 7 years after the date of their last assessment. All others will have to have either an updated assessment or initial assessment conducted as required by the standard.” Personnel who have not had a personnel risk assessment within the previous 7 years from the implementation date will need to have one on (or around) the implementation date of this standard. For a Responsible Entity that has not historically conducted any type of Personnel Risk Assessments or that has long-time employees without recent Personnel Risk Assessments, this could be a burdensome requirement.</p>
CIP-004-1	R3.1	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.		
CIP-004-1	R3.2	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.		
CIP-004-1	R3.3	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.		
CIP-004-1	R4	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	NERC 1207 – Personnel	<p>NERC CIP-004 Requirement 4 is closely linked to NERC 1207. The compliance program used for NERC 1207 should be able to address Requirement 4.</p> <p>NERC 1207 requires: “the responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s).”</p> <p>NERC 1207 requires: “The responsible entity shall review the document referred to in 1207.2.1 at least quarterly and update the document within 24 hours of any change.” While the new requirement is a bit more flexible in terms of frequency of</p>
CIP-004-1	R4.1	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-004-1	R4.2	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.		review and update, the documentation must still be scrupulously maintained. Also, Responsible Entities must preserve the capability to remove "access to Critical Cyber Assets within 24 hours for personnel terminated for cause." Responsible Entities should remember this requirement as they design processes and purchase equipment – since a centralized access control tool is likely the only way to reliably revoke access on a large number of Critical Cyber Assets within 24 hours.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-005-1 – Electronic Security Perimeter(s)</b>				
CIP-005-1	R1	Electronic Security Perimeter —The Responsible Entity shall identify the Electronic Security Perimeter(s) surrounding its Critical Cyber Assets and all access points to the perimeter(s).	1203 – Electronic Security Perimeter	NERC 1203 states: "The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s)." This is essentially the same requirement, except now the requirement is expanded in the following sub-requirements.
CIP-005-1	R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	No Reference Found	While this is a new requirement, this is a straightforward requirement. Obviously, the dial-up modems that terminate communication links should be considered access points to the Electronic Security Perimeter. Adequate filtering should be put in place on both the "in-band" interface and the administrative interface on these devices to properly enforce the Electronic Security Perimeter. This should not require too much time to implement properly.
CIP-005-1	R1.2	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	No Reference Found	This is a new requirement, and may be a challenge for large organizations. If an organization has many Critical Cyber Assets, they'll need to quickly identify any that are dial-up accessible, and implement an Electronic Security Perimeter for each one.
CIP-005-1	R1.3	Communication links connecting discrete electronic perimeters shall not be considered part of the security perimeter. However, end points of these communication links within the security perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	No Reference Found	While this is a new requirement, this is a straightforward requirement. Obviously, the routers that terminate communication links should be considered access points to the Electronic Security Perimeter. Adequate filtering should be put in place on both the "in-band" interface and the administrative interface on these devices to properly enforce the Electronic Security Perimeter. This should not require too much time to implement properly.
CIP-005-1	R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	No Reference Found	Another difference between NERC 1200 and NERC CIP is that NERC specifically chose to state that non-critical Cyber Assets within the perimeter "shall be identified and protected pursuant to the requirements of Standard CIP-005." This is very reasonable, since an insecure cyber asset within the electronic security perimeter could lead to the compromise of a Critical Cyber Asset. While this won't represent a problem for most utilities that chose to separate their business networks from their operational networks, it may be a significant burden for utilities that, for example, have dial-up accessible non-critical cyber assets within the Electronic Security Perimeter.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-005-1	R1.5	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	No Reference Found	This is a new requirement, and may be a challenge for large organizations. Cyber Assets that provide security services for the Electronic Security Perimeter(s) must now basically be inside the Electronic Security Perimeter(s).  This may represent a significant challenge for companies that are used to supporting an operational network and a business network using the same cyber assets. Those companies will have to duplicate the assets inside the perimeter, or move the assets inside the perimeter and have the undesirable task of supporting the business environment from within the operational network.
CIP-005-1	R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	1203 – Electronic Security Perimeter	NERC 1203 states: "The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s). The document shall verify that all critical cyber assets are within the electronic security perimeter(s)." The new requirement is very similar to the old requirement, and Responsible Entities should have no trouble demonstrating compliance.
CIP-005-1	R2	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	1204 – Electronic Access Controls	NERC 1204 requires Responsible Entities to: "identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter." The requirements under Requirement 2 extend the existing 1204 requirement, and will force Responsible Entities to carefully evaluate their Electronic Access Controls and improve a few specific things to demonstrate full compliance.
CIP-005-1	R2.1	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	1212 – Systems Management	NERC 1212 requires: "The disabling of unused network services and ports;" and that requirement is carried forward to NERC CIP-005 Requirement 2. This requirement reflects a "default deny" approach to security – certainly the recommended approach for something as serious as the security of the systems that ensure the reliable flow of electricity.  Admittedly, this requirement is in a bit of a different context than the requirement in NERC 1212, since NERC 1212 was focused on system security rather than perimeter security. It should not come as a surprise, however, and Responsible Entities should be able to demonstrate compliance quickly.
CIP-004-1	R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.		
CIP-004-1	R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	1212 – Systems Management	NERC 1212 requires using: "Secure dial-up modem connections" in the context of system security. Now, that must be extended to perimeter security. This will require some substantial effort, especially for large organizations that have a large number of Critical Cyber Assets and have previously used dial-up access for those assets.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-005-1	R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	No Reference Found	<p>While basically based on NERC 1204 – Electronic Access Controls, this requirement is stronger than anything in NERC 1200. It will require a Responsible Entity to “implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party” with the caveat “where technically feasible.”</p> <p>N&amp;ST expects that this requirement would be satisfied by some type of two-factor authentication system, or some system more sophisticated than a simple password scheme.</p> <p>If the Responsible Entity has no external interactive logical access through the Electronic Security Perimeter, this requirement becomes a non-issue. This requirement should encourage Responsible Entities to move towards the model where few accesses take place through the perimeter. This may not be possible, however, without significantly changing business processes and procedures – another large investment of time and money.</p> <p>While this is a new requirement, this should be straightforward for compliance. Since the requirement says: “where technically feasible”, Responsible Entities have some flexibility to only meet this requirement where it is actually possible – and they don’t have to upgrade or replace systems just to meet this requirement.</p>
CIP-004-1	R2.5	The required documentation shall, at least, identify and describe:	1204 – Electronic Access Controls	<p>NERC 1204 states: “The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).”</p> <p>While the document described by Requirement 2.5 was basically required by NERC 1204, the document must be heavily revised to address the specific requirements in this CIP document. Revising this document, however, should be able to be accomplished within a tight deadline.</p>
CIP-004-1	R2.5.1	The processes for access request and authorization.		
CIP-004-1	R2.5.2	The authentication methods.		
CIP-005-1	R2.5.3	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.		
CIP-005-1	R2.5.4	The controls used to secure dial-up accessible connections.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-005-1	R2.6	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	No Reference Found	While this is a new requirement, this should be straightforward for compliance. Since the requirement says: “where technically feasible”, Responsible Entities have some flexibility to only meet this requirement where it is actually possible – and they don’t have to upgrade or replace systems just to meet this requirement.
CIP-005-1	R3	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	1209 – Monitoring Electronic Access	NERC 1209 requires Responsible Entities to: “monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week” and to “maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned.” This is basically the same requirement, so NERC 1200 compliant Responsible Entities should have no trouble demonstrating compliance, but some of the sub-requirements will require significant attention to ensure compliance.
CIP-005-1	R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	No Reference Found	This is a new requirement. Responsible Entities will have to carefully consider what procedural and technological solutions will work in their environment. For a large Responsible Entity to fully comply with this requirement may require some significant effort, and Responsible Entities must consider whether future investments in dial-up access can be made compliant – and how valuable dial-up access is to their operational capability.
CIP-005-1	R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	No Reference Found	This is a new requirement, and slightly modifies the requirement above. This should reduce some of the burden faced by Responsible Entities for NERC CIP compliance.  This is partially addressed by a number of the NERC 1200 standards, including NERC 1209 and NERC 1212, but is basically a new requirement. Reviewing access logs can be a challenging task because the access logs on a busy cyber asset can be voluminous. Responsible Entities would be wise to implement some automated techniques for reviewing the access log files and meeting this requirement, since manual processes are not likely to be realistic on busy systems.
CIP-005-1	R4	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	1212 – Systems Management	NERC 1212 requires Responsible Entities to have procedures addressing: “identification of vulnerabilities and responses.”  The sub-requirements in this section basically ensure that the vulnerability assessment program from NERC 1212 is extended to the Electronic Security Perimeter(s).
CIP-005-1	R4.1	A document identifying the vulnerability assessment process;		While this is basically the same requirement from NERC 1212, Responsible Entities will have to evaluate their vulnerability

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-005-1	R4.2	A review to verify that only ports and services required for operations at these access points are enabled;		assessment program and ensure that it addresses all of the sub-requirements mentioned here and can be extended to include the Electronic Security Perimeter(s).
CIP-005-1	R4.3	The discovery of all access points to the Electronic Security Perimeter;		
CIP-005-1	R4.4	A review of controls for default accounts, passwords, and network management community strings; and,		
CIP-005-1	R4.5	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.		
CIP-005-1	R5	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	1204 – Electronic Access Controls	NERC 1204 requires: "The responsible entity shall review and update the documentation referenced in 1204.2.1 at least annually or within 90 days of the modification of the electronic security perimeter or the electronic access controls." This requirement is essentially the same, so NERC 1200 compliant Responsible Entities should have no trouble demonstrating compliance.
CIP-005-1	R5.1	The Responsible Entity shall ensure that all documentation required by Standard CIP- 005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.		
CIP-005-1	R5.2	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.		
CIP-005-1	R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-006-1 – Physical Security of Critical Cyber Assets</b>				
CIP-006-1	R1	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	No Reference Found	NERC 1200 required individual documents on the perimeter, access controls and monitoring – NERC CIP now requires a document that includes all of these aspects of physical security. If the Responsible Entity created appropriate documents to address NERC 1200 compliance requirements, it should be possible to combine those documents together in to a physical security plan.
CIP-006-1	R1.1	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	NERC 1205 – Physical Security Perimeter	NERC 1205 states: “The responsible entity shall maintain a document depicting the physical security perimeter(s) and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeter(s).”  The new requirement is essentially the same, with additional definition of what constitutes a physical perimeter. Responsible Entities now have more flexibility (although a stricter “six wall” requirement), since the physical perimeter does not have to be a room – it can simply be a locked cage or cabinet within the room. Any Responsible Entity that defined their physical perimeter for NERC 1200 compliance should have no trouble meeting the requirement for NERC CIP compliance, unless their physical perimeter did not include six walls (or alternative measures) – which could introduce significant compliance challenges.
CIP-006-1	R1.2	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	1206 – Physical Access Controls	NERC 1206 states: “The responsible entity shall maintain a document identifying the access controls and their implementation for each physical access point to the physical security perimeter(s).” In this case, the new requirement is basically the same as the old requirement.
CIP-006-1	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	1208 – Monitoring Physical Access	NERC 1208 states: “The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are functioning and being used as planned.” The new requirement is slightly simpler than the old requirement, since the new requirement does require verifying that the tools and procedures are being used as planned. There should be no major gap here for NERC CIP compliance.
CIP-006-1	R1.4	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	No Reference Found	This specific requirement does not come from a similar requirement in NERC 1200. This requirement was most likely addressed, however, when the responsible entity addressed physical access controls, and should be easy for Responsible Entities to include in their physical security plan.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-006-1	R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	NERC 1207 – Personnel	NERC 1207 requires: "the responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s)." Responsible Entities will have to document the processes associated with creating this list, which extends the NERC 1207 requirement slightly.
CIP-006-1	R1.6	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	No Reference Found	This is a new requirement. Although escorted access has been part of physical security for Critical Cyber Assets for a long time, documenting the procedures is a new requirement.
CIP-006-1	R1.7	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	NERC 1205 – Physical Security Perimeter	NERC 1205 states: "The responsible entity shall review and update the document referenced in 1205.2.1 at least annually or within 90 days of the modification of the network." This requirement refers to the "document depicting the physical security perimeter(s) and all physical access points to every such perimeter."  Since this is essentially the same requirement, with a bit of an expanded scope, it shouldn't impose a significant compliance burden for Responsible Entities.
CIP-006-1	R1.8	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	No Reference Found	This is a new requirement. While the Cyber Assets "used in the access control and monitoring of the Physical Security Perimeter(s)" do not need to be within the Electronic Security Perimeter, they must be part of the overall security program (including personnel risk assessments for users), and must have electronic access controls, electronic monitoring, physical access controls, physical monitoring, system security controls, incident response and recovery plans.  Responsible entities that bought "off the shelf" systems for physical security, and have those systems controlled by other personnel (including contractors) will need to consider how those systems are protected. Due to the (occasionally) divergent nature of electronic and physical security, meeting this requirement may require some effort.
CIP-006-1	R1.9	Process for ensuring that the physical security plan is reviewed at least annually.	NERC 1205 – Physical Security Perimeter	NERC 1205 states: "The responsible entity shall review and update the document referenced in 1205.2.1 at least annually or within 90 days of the modification of the network." This requirement refers to the "document depicting the physical security perimeter(s) and all physical access points to every such perimeter."  Since this is essentially the same requirement, with a bit of an expanded scope, it shouldn't impose a significant compliance burden for Responsible Entities.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-006-1	R2	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	NERC 1205 – Physical Security Perimeter	Beyond the documentation requirement above, NERC CIP now requires actual implementation of controls to manage physical access following a risk assessment procedure. While generally based on NERC 1206, this is a bit more complex. There are specific requirements to use one or more of the access control methods described within this requirement.
CIP-006-1	R2.1	Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another..		Responsible Entities must now assess their perimeter to ensure that adequate access controls are implemented. If the access controls are found to be insufficient, the Responsible Entity must quickly implement one or more of the physical access control methods described in the requirement. Implementing any of these access control solutions can be expensive, and can be particularly difficult to do in a wide variety of facilities on a short timeframe. Responsible Entities need to start planning early for controlling physical access to Critical Cyber Assets.
CIP-006-1	R2.2	Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.:		
CIP-006-1	R2.3	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.		
CIP-006-1	R2.4	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.		
CIP-006-1	R3	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	1208 – Monitoring Physical Access	Beyond the documentation requirement above, NERC CIP now requires actual implementation of controls to monitor physical access following a risk assessment procedure. Since the NERC 1208 requirement specifically required “24 by 7” monitoring, complying with this requirement should not require a reengineering of physical access control monitoring at facilities subject to the NERC 1200 standard.
CIP-006-1	R3.1	Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.		If the monitoring techniques in place are insufficient, the Responsible Entity must quickly implement one or more of the physical access monitoring methods described in the requirement. Implementing any of these monitoring solutions can be expensive, and can be particularly difficult to do in a wide variety of facilities on a short timeframe. Responsible Entities need to start planning early for controlling physical access to Critical Cyber Assets.
CIP-006-1	R3.2	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.		
CIP-006-1	R4	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	1208 – Monitoring Physical Access	NERC 1208 states: “The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring.” Since the new requirement only requires “technical and procedural mechanisms for logging”, NERC 1200 compliant Responsible Entities already comply with this

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-006-1	R4.1	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.		requirement at facilities subject to the NERC 1200 standard.
CIP-006-1	R4.2	Video Recording: Electronic capture of video images of sufficient quality to determine identity.		At other facilities, and for Responsible Entities who were not required to meet the NERC 1200 standard, one of the logging methods described here must be implemented. Implementing any of these logging solutions can be expensive, and can be particularly difficult to do in a wide variety of facilities on a short timeframe. Responsible Entities need to start planning early for controlling physical access to Critical Cyber Assets.
CIP-006-1	R4.3	Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.		
CIP-006-1	R5	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	1208 – Monitoring Physical Access	
CIP-006-1	R6	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	No Reference Found	This is a new requirement – maintenance and testing for monitoring equipment was not included in NERC 1200. Compliance with this requirement will necessitate some extra effort by Responsible Entities to ensure they are adequately maintaining (and documenting the maintenance on) physical security equipment.
CIP-006-1	R6.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.		
CIP-006-1	R6.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.		
CIP-006-1	R6.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-007-1 – Systems Security Management</b>				
CIP-007-1	R1	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	1213 – Test Procedures	NERC 1213 requires that Responsible Entities: “shall establish test procedures and acceptance criteria to ensure that critical cyber assets installed or modified comply with the security requirements in this standard. Test procedures shall require that testing and acceptance be conducted in an isolated test environment.”  The new requirement is similar but more specific. Now, NERC CIP identifies minimum baseline of “significant changes” that must use the test procedures: “implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.”
CIP-007-1	R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.		NERC CIP no longer specifically requires an isolated test environment, however. As long as the Responsible Entity’s test procedures “minimizes adverse effects on the production system or its operation” an isolated test environment is no longer specifically required. Obviously, an isolated test environment “that reflects the production environment” is the best way to ensure test procedures do not affect the production environment. If that is not possible or reasonable, a Responsible Entity can use procedures to ensure the test doesn’t affect the production environment.
CIP-007-1	R1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.		
CIP-007-1	R1.3	The Responsible Entity shall document test results.		
CIP-007-1	R2	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	1212 – Systems Management	Managing unused ports and services is one aspect of systems management that is discussed in NERC 1212. Specifically, NERC 1212 requires Responsible Entities to: “establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address...the disabling of unused network services and ports.”  The new requirement in NERC CIP is quite a bit more sophisticated and specific, however, which will require Responsible Entities to examine their current practices and possibly adjust them to meet the NERC CIP requirements.
CIP-007-1	R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.		
CIP-007-1	R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).		
CIP-007-1	R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-007-1	R3	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	1212 – Systems Management	Security Patch Management is one aspect of systems management that is discussed in NERC 1212. Specifically, NERC 1212 requires Responsible Entities to: “establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address...security patch management.”
CIP-007-1	R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.		The new requirement in NERC CIP is quite a bit more sophisticated and specific, however, which will require Responsible Entities to examine their current practices and possibly adjust them to meet the NERC CIP requirements.
CIP-007-1	R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.		
CIP-007-1	R4	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	1212 – Systems Management	This requirement has been expanded from “Anti-Virus Software” to “Malicious Software Prevention” but the goal remains the same. Responsible Entities must use software to prevent systems from being compromise by “malware” and to prevent malware from spreading within the Electronic Security Perimeter(s).
CIP-007-1	R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.		In NERC 1200, this was known as anti-virus software, and it is one aspect of systems management that is discussed in NERC 1212. Specifically, NERC 1212 requires Responsible Entities to: “establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address... The installation and update of anti-virus software.”
CIP-007-1	R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures		
CIP-007-1	R5	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	1204 – Electronic Access Controls <b>And</b> 1209 – Monitoring Electronic Access <b>And</b> 1212 – Systems Management	This is a complex requirement with many subparts. Parts of this were addressed in NERC 1204, NERC 1209 and NERC 1212, but other parts are new requirements for Responsible Entities to address. Each part is discussed below.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-007-1	R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.		Portions of this requirement come from NERC 1204 and NERC 1212, but other parts are new requirements. Either way, the requirements are much more detailed than any requirements from NERC 1200.
CIP-007-1	R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	1204 – Electronic Access Controls	NERC 1212 requires Responsible Entities to: "establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address...The authorization and periodic review of computer accounts and access rights." Particularly enthusiastic Responsible Entities may have addressed this sufficiently to address Requirement 5.1.1 and Requirement 5.1.3, but those policies procedures should be carefully reviewed to ensure they meet the specific requirements here.
CIP-007-1	R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	And 1212 – Systems Management	Requirement 5.1.2 and may pose a significant challenge. NERC 1209 addressed aspects of Requirement 5.1.2, but are likely not sufficient for compliance. Previously, per NERC 1209: "the responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights." Now Critical Cyber Assets must create "historical audit trails of individual user account access activity for a minimum of ninety days."
CIP-007-1	R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	And 1209 – Monitoring Electronic Access  And No Reference Found	With the requirement for audit trails of "individual user account access activity" it is clear that this is a significantly larger requirement. Moreover, this requirement may have been ignored in the past because many control system software packages and embedded software packages on Critical Cyber Assets are not configured to support this level of logging. While Responsible Entities are not required to replace systems to meet this requirement, they must reconfigure existing systems and use this Requirement as a purchasing criterion in the future. This requirement may change business process (requiring individual login accounts) and change technology decisions. Responsible Entities should consider this requirement particularly carefully.
CIP-007-1	R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	1212 – Systems Management	Portions of this requirement come from NERC 1204 and NERC 1212, but other parts are new requirements. Either way, the requirements are much more detailed than any requirements

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-007-1	R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	And  No Reference Found	from NERC 1200.  NERC 1212 requires Responsible Entities to: "establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address...default passwords for newly installed equipment."  While enthusiastic Responsible Entities may have addressed these requirements in their NERC 1200 program, all Responsible Entities will have to carefully review and update their procedures for administrator, shared, and other generic account privileges. N&ST believes it is unlikely that Responsible Entities have addressed all of these requirements, including identifying individuals with access to shared accounts and putting compensating controls in place around those accounts.
CIP-007-1	R5.2.2	The Responsible Entity shall identify those individuals with access to shared accounts.		
CIP-007-1	R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).		
CIP-007-1	R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	No Reference Found	Like other parts of Requirement 5, Requirement 5.3 significantly extends NERC 1200. In this case, Requirement 5.3 lays out explicit rules for passwords. In the past, Responsible Entities may have used passwords – but it is unlikely that that consistently used passwords that met these rules. This requirement may change business process (how passwords are generated) and change technology decisions. Responsible Entities should consider this requirement particularly carefully.
CIP-007-1	R5.3.1	Each password shall be a minimum of six characters.		
CIP-007-1	R5.3.2	Each password shall consist of a combination of alpha, numeric, and "special" characters.		
CIP-007-1	R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.		
CIP-007-1	R6	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	1209 – Monitoring Electronic Access  And  1212 – Systems Management  And  No Reference Found	This requirement significantly extends both NERC 1209 and NERC 1212.  NERC 1209 required: "The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs)." Access is certainly a system event that is related to cyber security, so Responsible Entities are likely addressing this portion of the requirement.  System Log Monitoring is one aspect of systems management that is discussed in NERC 1212. Specifically, NERC 1212 requires Responsible Entities to: "establish systems management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address..." "The retention and review of operator logs, application logs, and intrusion detection logs."
CIP-007-1	R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	No Reference Found	
CIP-007-1	R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-007-1	R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008.		<p>The new requirement in NERC CIP is quite a bit more sophisticated and specific. It will require Responsible Entities to examine their current practices and possibly adjust them to meet the NERC CIP requirements.</p> <p>Maintaining, retaining and reviewing logs of system events related to cyber security may be a challenging requirement to meet. Log files are often voluminous, and reviewing them on a regular basis will be challenge for personnel who are already fully deployed. Technical mechanisms (automated tools) are often expensive and complex, requiring extensive system integration effort.</p> <p>Additional staff may be required to set up the Security Status Monitoring capability, monitor “alerts for detected Cyber Security Incidents,” “review logs of system events related to cyber security,” and “maintain records documenting review of logs.”</p> <p>Due to the requirement for additional procedures and tools, Responsible Entities should carefully consider CIP-007 Requirement 6 and ensure they are planning for compliance.</p>
CIP-007-1	R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.		
CIP-007-1	R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.		
CIP-007-1	R7	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	No Reference Found	<p>This is a new requirement. Conscientious Responsible Entities may do this already, although it is more likely that this requirement is not met – or that equipment is stored rather than being redeployed or disposed!</p> <p>Responsible Entities may have to work with various internal groups (and potentially subcontractors) who handle equipment disposal and redeployment to ensure this requirement is met (and appropriate documentation is created).</p> <p>The best way to ensure compliance with this requirement is for internal staff to handle the erasure or destruction of storage media – but internal staff are likely already busy, and this requirement will place an additional burden on them. Because of this, Responsible Entities should start planning for how they are going to meet this requirement and document their compliance.</p>
CIP-007-1	R7.1	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.		
CIP-007-1	R7.2	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.		
CIP-007-1	R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.		
CIP-007-1	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:		

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-007-1	R8.1	A document identifying the vulnerability assessment process;		<p>and responses.” While the old requirement is very general, it is the same notion as CIP-007 Requirement 8.</p> <p>Responsible Entities must now complete a vulnerability assessment that, at a minimum, includes a review of:</p> <ol style="list-style-type: none"> <li>1. Ports and services, and</li> <li>2. Controls for default accounts.</li> </ol> <p>The vulnerability assessment process must now be documented and the outcome of the assessment must be documented. In fact, the output must specifically include: “the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.”</p> <p>Responsible Entities will have to carefully examine the vulnerability assessment program created for NERC 1212 compliance, and ensure that the program is sufficient for compliance with CIP-007 Requirement 8.</p>
CIP-007-1	R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;		
CIP-007-1	R8.3	A review of controls for default accounts; and,		
CIP-007-1	R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.		
CIP-007-1	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	1212 – Systems Management	NERC 1212 does require Responsible Entities to create and maintain documentation about systems management. This requirement is generally equivalent to the requirement in NERC 1212.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-008-1 – Incident Reporting and Response Planning</b>				
CIP-008-1	R1	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	<p>NERC 1214 – Electronic Incident Response Actions</p> <p>And</p> <p>NERC 1215 – Physical Incident Response Actions</p>	<p>NERC 1214 required that “the responsible entity shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.” The new requirement includes an “incident response plan” – a much larger requirement than the requirement in NERC 1214. Responsible Entities will have to carefully evaluate the documentation created for NERC 1214 compliance and ensure that it addresses “assessing, mitigating, containing, reporting and responding to Cyber Security Incidents.”</p> <p>The Responsible Entity should also consider the physical incident response document created for NERC 1215 compliance. This document is no longer needed, but it may include portions to be included in the new incident response plan required for compliance.</p>
CIP-008-1	R1.1	Procedures to characterize and classify events as reportable Cyber Security Incidents.		This is a new requirement. Incident classification was not part of the NERC 1214 requirement, but may have been accomplished by organizations that built aggressive incident response programs. If not, an incident classification system will have to be built and deployed.
CIP-008-1	R1.2	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.		NERC 1214 requires only that the responsible entity “shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.” This is an important part of the new requirement, but it does not satisfy the entire requirement. Responsible Entities must now create much more documentation for full compliance, including incident handling procedures and communications plans.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-008-1	R1.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.		NERC 1214 requires: "The document in 1214.2.1 shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure."  Responsible Entities must evaluate their incident response plans to ensure they accurately reflect the requirements of the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). Since this type of notification was the previous requirement, it should already be adequately documented, but it must be reviewed in light of any new guidance from the Indications, Analysis & Warning Program.
CIP-008-1	R1.4	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.		NERC 1214 stated that: "Electronic incident response plan exists, but has not been reviewed or updated in the last 12 months" constituted "level one" non-compliance. While this is basically the same requirement, Responsible Entities must now update the Cyber Security Incident response plan "within ninety calendar days of any changes." This will cause some additional challenges for Responsible Entities, but should be a reasonable expectation.
CIP-008-1	R1.5	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.		
CIP-008-1	R1.6	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	No Reference Found	This is a new requirement. Responsible Entities must now test their Cyber Security Incident response plan annually. While this is a new requirement, Responsible Entities should be able to comply within the first year of the implementation plan deadline.
CIP-008-1	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	NERC 1214 – Electronic Incident Response Actions  And  NERC 1215 – Physical Incident Response Actions	NERC 1214 and NERC 1215 required Responsible Entities to keep data for three calendar years. It's logical that Responsible Entities keep records related to Cyber Security Incidents, since they may be needed by investigators and prosecutors.  The new requirement has the same time requirement.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
<b>NERC CIP-009-1 – Recovery Plans for Critical Cyber Assets</b>				
CIP-009-1	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	NERC 1216 – Recovery Plans	NERC’s 1200 standards address parts of CIP-009, but CIP-009 is more specific and extends beyond the requirements in NERC 1200. For example, creating a recovery plan and exercising it annually is required for NERC 1200 compliance, but NERC 1216 does not discuss change communication or the backup and storage of information required to successfully restore Critical Cyber Assets.  NERC 1216 states: “The plans and procedures shall define roles and responsibilities by individual or job function.” Since Requirement 1.2 was part of NERC 1216, Responsible Entities should already be compliant. Requirement 1.1 is a more specific logical extension of NERC 1216.
CIP-009-1	R1.1	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).		
CIP-009-1	R1.2	Define the roles and responsibilities of responders.		
CIP-009-1	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	NERC 1216 – Recovery Plans	NERC 1216 states that Responsible Entities “shall create action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Each responsible entity shall exercise these plans at least annually.” NERC 1216 also states: “The responsible entity shall maintain a document verifying that the action plan is exercised via drill at least annually.” The new requirement is even more specific, requiring Responsible Entities to update their recover plans after each exercise. This is a reasonable requirement, however, and Responsible Entities should have plenty of time to comply.
CIP-009-1	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	NERC 1211 – Training	NERC 1211 states “the training shall address, at a minimum... action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.”  It is likely that Responsible Entities already include some aspects of recovery in the training created for NERC 1211. When the plans are updated, however, Responsible Entities must quickly review the training and awareness materials and redistribute them to the responsible personnel.

Standard	Req #	Requirement Text	NERC 1200 Standard	Comments
CIP-009-1	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No Reference Found	This is a new requirement. This was not included in NERC 1216 – Recovery Plans. This is a logical requirement, however, and conscientious Responsible Entities likely already have “processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.” Responsible Entities must evaluate whether they already have these processes and procedures, and if not, they must be created quickly for NERC CIP compliance.
CIP-009-1	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	No Reference Found	This is a new requirement. This was not included in NERC 1216 – Recovery Plans. This is a logical requirement, however, and conscientious Responsible Entities likely already have processes for testing backup media. Responsible Entities must evaluate whether they already have these processes and procedures, and if not, they must be created quickly for NERC CIP compliance.

## Bibliography

### **NERC 1200**

North American Electric Reliability Council. "Urgent Action Standard 1200 – Cyber Security." August, 2005. North American Electric Reliability Council 26 January 2006.

[http://www.nerc.com/~filez/standards/Cyber\\_Sec\\_Renewal.html](http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html)

North American Electric Reliability Council. "Implementation Plan Second Renewal of Urgent Action Cyber Security Standard." June 1, 2005. North American Electric Reliability Council 26 January 2006.

[http://www.nerc.com/~filez/standards/Cyber\\_Sec\\_Renewal.html](http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html)

North American Electric Reliability Council. "Implementation Plan – Renewal of Urgent Action Cyber Security Standard." June 2, 2004. North American Electric Reliability Council 26 January 2006.

[http://www.nerc.com/~filez/standards/Cyber\\_Sec\\_Renewal.html](http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html)

### **NERC CIP Draft 4**

North American Electric Reliability Council. "CIP-002-1" through "CIP-009-1", Draft 4. January, 2006. North American Electric Reliability Council 26 January 2006. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

North American Electric Reliability Council. "Cyber Security Implementation Plan." January, 2006. North American Electric Reliability Council 26 January 2006. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

North American Electric Reliability Council. "Frequently Asked Questions (FAQs) Cyber Security Standards CIP-002-1 through CIP-009-1." January, 2006. North American Electric Reliability Council 26 January 2006. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

### **NERC CIP Draft 3**

North American Electric Reliability Council. "CIP-002-1" through "CIP-009-1", Draft 3. May, 2005. North American Electric Reliability Council 10 May

2005. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

North American Electric Reliability Council. "Cyber Security Implementation Plan." May, 2005. North American Electric Reliability Council 10 May 2005. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

North American Electric Reliability Council. "Frequently Asked Questions (FAQ's) Cyber Security Standards CIP-002-1 through CIP-009-1." May, 2005. North American Electric Reliability Council 10 May 2005. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

### ***NERC CIP Draft 2***

North American Electric Reliability Council. "CIP-002-1" through "CIP-009-1", Draft 2. January, 2005. North American Electric Reliability Council 18 Mar 2005. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

North American Electric Reliability Council. "Cyber Security Implementation Plan." January, 2005. North American Electric Reliability Council 18 Mar 2005. <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

### ***Other Documents***

U.S.-Canada Power System Outage Task Force. "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." April 2004.