
NERC Cyber Security Standards, CIP-002-1 through CIP-009-1: Compliance Reference

December 12, 2006

Prepared By:

Network & Security Technologies
161 North Middletown Road
Pearl River, NY 10965-2029
Phone: (845) 620-9500
<http://www.netsectech.com>



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

Network & Security Technologies, Inc. (N&ST) has prepared this white paper to help electric utility companies (known as Responsible Entities in the standards) with their compliance efforts for the new NERC Cyber Security Standards, CIP-002-1 through CIP-009-1. The NERC Cyber Security Standards (NERC CSS) include 41 separate requirements (and over a hundred sub-requirements) that make compliance challenging for all Responsible Entities. The measures required by these standards ensure the security and reliability of the Bulk Electric System by protecting the Cyber Assets essential to the operation of Critical Assets – the Critical Cyber Assets.

While working with our clients on their NERC CSS compliance programs, N&ST has recognized the need for a concise reference to the standards. Such a reference will help Responsible Entities apportion responsibility for defining and documenting required security-related policies and procedures, understand how to review and retain that documentation, and enumerate time-sensitive requirements for compliance. N&ST originally prepared this quick reference document for its clients, but released it to assist other companies in the industry with their own compliance efforts.

This document addresses multiple types of Critical Assets: control centers, substations and generating units. For the Responsible Entities, some requirements in the CSS typically need enterprise-wide efforts, others need business unit level effort, and still others need a per-Critical Asset approach.

Of course, the differences between Responsible Entity organizational structures and technical feasibility mean that every compliance program will be unique. For example, one Responsible Entity may have a business-unit-wide program for Systems Security Management (CIP-007) of Cyber Assets at all of its generating plants while another may require each generating plant to develop its own CIP-007 compliance program. As Responsible Entities review this white paper, they should keep in mind that while the assignments presented may need tailoring to their specific environment, the requirements for retaining, reviewing and updating documentation apply to all Responsible Entities and must be addressed somewhere in their organization.

N&ST hopes this white paper will prove a useful reference for Responsible Entities undertaking the challenge of securing their Critical Cyber Assets. The industry's reliability standards reflect the interconnected nature of the North American electric power system. All Responsible Entities must take cyber security seriously to ensure the continued availability of a reliable Bulk Electric System.

About This White Paper

This white paper presents a table that lists the 41 separate requirements defined by the eight CIP standards. For each requirement, the table:

- Identifies the personnel that will most likely be responsible for compliance documentation within the Responsible Entity, including:
 - An enterprise-wide compliance group,
 - Personnel from a business unit, or
 - Personnel dedicated to operation of a particular Critical Asset.
- Lists specific document retention periods,
- Describes the review and update measures,
- Identifies time-sensitive activities needed under certain circumstances.

This document is intended primarily for Responsible Entities who are asset owners. These Responsible Entities will likely have business units or individual assets that operate autonomously yet must participate in an enterprise-wide compliance effort. For example, while a business unit may establish uniform standards for Critical Assets such as substations and generating plants, documentation to meet certain requirements will still need an asset-by-asset effort. The table in this document identifies the level at which compliance documentation must be created: at the Enterprise level, the business unit level or for each individual Critical Asset. However, the appropriate owner of compliance responsibility will depend upon the Responsible Entity's organizational structure.

The format of the CIP standards includes a section that addresses Compliance (Section D). Subsection 1.3 of that section, called "Data Retention", lists the data retention requirements for that standard. Unless specified otherwise for specific requirements or documents, the standard typically states: "The Responsible Entity shall keep all documentation and records from the previous full calendar year." That means that as of December of any given year, the Responsible Entity should have almost two full years of documentation and records available for an auditor to review.

Compliance Documentation Requirements

The dark gray cells in the table below indicate the most likely group of personnel within the Responsible Entity that is accountable for compliance with the NERC CSS requirement. The light grey cells represent where other personnel will need to also produce documentation or records to demonstrate compliance. The final columns indicate the retention period and update frequency for compliance documentation as well as other time-sensitive requirements.

NERC Standard	CIP Requirement	Responsible Personnel			Documentation Retention Periods	Review, Update & Time-sensitive Requirements
		Enterprise Wide	Business Unit	Critical Asset		
CIP-002-1: Critical Cyber Asset Identification	R1 Critical Asset Identification Method				Previous full calendar year.	Annually review.
	R2 Critical Asset Identification					Annually review.
	R3 Critical Cyber Asset Identification					Annually review.
	R4 Annual Approval	Of Critical Asset list	Of Critical Cyber Asset lists	Of Critical Cyber Asset lists		Annually approve.
CIP-003-1: Security Management Controls	R1 Cyber Security Policy				Previous full calendar year.	Annually review.
	R2 Leadership (for adherence to NERC CIP standards)					Document change to Senior Manager within 30 days.
	R3 Exceptions (to the Cyber Security Policy)					Document within 30 days of approval & annually review.
	R4 Information Protection (protect based on sensitivity)					Annually assess adherence.
	R5 Access Control (to protected Critical Cyber Asset information)					Annually review: - list of authorizers; - access privileges; & - access control processes
	R6 Change Control and Configuration Management					
CIP-004-1: Personnel and Training	R1 Awareness (of cyber security)				Previous full calendar year.	Reinforce quarterly.
	R2 Training (program for cyber security)					1) Annually review program. 2) Train personnel within 90 days of authorization. 3) Annually conduct training.
	R3 Personnel Risk Assessment (employees and contractors)				In accordance with federal, state, provincial, and local laws.	1) Assess within 30 days of authorization 2) Re-assess every 7 years.
	R4 Access (create & maintain lists of authorized personnel)				Previous full calendar year.	1) Review quarterly and update list within 7 days. 2) Revoke access within: - 24 hours for personnel terminated for cause; - 7 days for personnel no longer requiring access.
CIP-005-1: Electronic Security Perimeter(s)	R1 Electronic Security Perimeter (around Critical Cyber Assets)				Previous full calendar year.	1) If no electronic alerting, assess logs every 90 days. 2) Annually assess cyber vulnerability.
	R2 Electronic Access Controls					1) 90 cal. days. 2) 3 calendar years if related to cyber incident.
	R3 Monitoring Electronic Access (to detect unauthorized access)					3) All CIP-005 doc'n: Annual review; update within 90 days of change.

NERC Standard	CIP Requirement	Responsible Personnel			Documentation Retention Periods	Review, Update & Time-sensitive Requirements
		Enterprise Wide	Business Unit	Critical Asset		
	R4 Cyber Vulnerability Assessment (of access points)				Previous full calendar year.	
	R5 Documentation Review and Maintenance					
CIP-006-1: Physical Security of Critical Cyber Assets	R1 Physical Security Plan (document perimeter & access points)				1) Access logs – 90 calendar days. 2) Incident logs – 3 calendar years. 3) Testing & maintenance records – 3 years. 4) Outage records – 1 calendar year. 5) Other – prev. full calendar year.	1) Update Physical Security Plan within 90 days of change. 2) Annually review Phys. Security Plan. 3) Perform testing and maintenance every 3 years.
	R2 Physical Access Controls (at all access points 24x7)					
	R3 Monitoring Physical Access (at all access points 24x7)					
	R4 Logging Physical Access (to uniquely identify user access)					
	R5 Access Log Retention					
	R6 Maintenance and Testing (of physical security systems)					
CIP-007-1: Systems Security Management	R1 Test Procedures (for upgrades to Cyber Assets within ESP)				Previous full calendar year.	Document patch assessment within 30 days of availability.
	R2 Ports and Services (enable only those required)					
	R3 Security Patch Management (track, evaluate, test & install)					
	R4 Malicious Software Prevention (for systems within ESP)					
	R5 Account Management (access authentication, accountability)				User account activity logs for 90 days (minimum).	1) Review user account privileges at least annually. 2) Change passwords at least annually.
	R6 Security Status Monitoring (of cyber security system events)				1) 90 cal. days. 2) 3 calendar years if related to cyber incident.	
	R7 Disposal or Redeployment (of Cyber Assets within the ESP)				Previous full calendar year.	Annually assess cyber vulnerability. All CIP-007 doc'n: Annual review; update within 90 days of change.
	R8 Cyber Vulnerability Assessment (Cyber Assets within ESP)					
	R9 Documentation Review and Maintenance					
CIP-008-1: Incident Reporting & Response Planning	R1 Cyber Security Incident Response Plan (classify reportable incidents, define response actions, report incidents to ES ISAC)				Previous full calendar year.	Annually review; annually test; update within 90 days of any changes.
	R2 Cyber Security Incident Documentation				3 calendar years.	
CIP-009-1: Recovery Plans for Critical Cyber Assets	R1 Recovery Plans				Previous full calendar year.	Annually review.
	R2 Exercise (of the Recovery Plan,)					Annually exercise the plan.
	R3 Change Control (of the Recovery Plan)					Communicate updates to Recovery Plan(s) within 90 calendar days.
	R4 Backup and Restore (Critical Cyber Asset information)					
	R5 Testing Backup Media (on-site or off-site)					Annually test that backup information is available.

About N&ST

Network & Security Technologies, Inc. is widely recognized as the premier expert in helping organizations achieve compliance with the NERC CSS. Many of the largest electric utilities have already chosen N&ST to assist them in ensuring the security of their Critical Cyber Assets. N&ST participated in programs to protect Critical Cyber Assets before the creation of NERC's interim Cyber Security Standard (NERC 1200), helped companies with NERC 1200 compliance, and has already performed numerous projects to aid companies with NERC CIP compliance.

N&ST is based in Pearl River, New York and has employees in seven states. Founded in 2003 by a group of senior information technology consultants, N&ST specializes in helping the electric power industry with networking, network security and regulatory compliance issues. With a focus on developing repeat clients by exceeding client expectations during every project, N&ST has created a sustainable and independent consulting business. N&ST is product-neutral and does not represent any vendors. Its team of expert consultants prides itself on creating practical and elegant solutions for its clients' most challenging problems.

Credits

N&ST is proud of its team of expert employees, and many N&ST team members played a role in creating this white paper. Patricia Meara developed the original table and did much of the work to create this paper. Michael Jacobs, Roger Fradenburgh, Nick Lauriat, Pete Nelson, Jeff Kimmelman and Adam Lipson all participated in reviewing this white paper and preparing it for publication.