



LogLogic® Compliance Suite: NERC Edition

NERC / FERC Background

The North American Electric Reliability Corporation (NERC) is a non-government organization with statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical, and efficient practices. As the federally designated Electric Reliability Organization (ERO) in North America, NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the NERC Critical Infrastructure Protection (CIP) Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or effect the reliability of North America's bulk electric systems.

In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability Standards proposed by NERC, making the NERC CIP Cyber Security Standards mandatory and enforceable across all users, owners, and operators of the bulk-power system.

The implementation plan can be accessed at Reliability Standards section of the NERC site. Click Critical Infrastructure Protection (CIP); under CIP-002-1, Critical Cyber Asset Identification, find the Implementation Plan.

Overview of NERC CIP Standards

The NERC CIP Cyber Security Standards require bulk power suppliers to define methods, processes, and procedures for securing critical cyber assets, as well as the non-critical cyber assets within the electronic security perimeter. NERC CIP standards are broad and cover a number of procedural and technical aspects of securing critical infrastructure. The LogLogic® Compliance Suite: NERC Edition offers capabilities to help meet the NERC CIP standards, as summarized in the table below.

Standard	Short Description	LogLogic Compliance Suite: NERC Edition Capabilities
CIP 001 – Sabotage Reporting	Standard CIP-001 requires Responsible Entities to report disturbances or unusual occurrences, suspected or determined to be caused by sabotage, to the appropriate systems, governmental agencies, and regulatory bodies.	LogLogic® Open Log Management and LogLogic® Security Event Management solutions can help gather the necessary forensic evidence to complete the reporting.
CIP 002 – Critical Cyber Assets	Standard CIP-002 requires Responsible Entities to identify and document Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.	LogLogic® Open Log Management and LogLogic® Security Event Management solutions can monitor the critical cyber assets as prescribed.
CIP 003 – Security Management Controls	Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.	LogLogic® Open Log Management and LogLogic® Security Event Management solutions assist in monitoring geographically distributed information systems 24x7 using the built-in alerting and notification modules. The NERC Edition of the LogLogic® Compliance Suite provides a summary or detailed report as needed to support this activity.

Standard	Short Description	LogLogic Compliance Suite: NERC Edition Capabilities
CIP 004 – Personnel and Training	Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.	LogLogic® Open Log Management and LogLogic® Security Event Management solutions can help track the access to various critical assets identified and classified that violates the defined policies in the system.
CIP 005 – Electronic Security	Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.	LogLogic® solutions provide the collection, analysis, reporting, alerting, and archiving of enterprise system and activity logs from all access points. The NERC Edition of the LogLogic® Compliance Suite provides a summary or detailed report as needed to review or report on these activities.
CIP 006 – Physical Security	Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.	(This control requires entities to implement physical security systems. Industry standards include the NIST FIPS 201 and HSPD 12 programs.)
CIP 007 – Systems Security Management	Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).	LogLogic® Open Log Management, LogLogic® Change Management and LogLogic® Security Event Management solutions can help review that the security methods, processes, and procedures for change control, system or user activities defined are enforced.
CIP 008 – Incident Reporting & Response Management	Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.	LogLogic® Open Log Management and LogLogic® Security Event Management solutions can be configured to integrate with existing incident management and reporting systems.
CIP 009 – Recovery Plans	Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.	LogLogic® Open Log Management solutions can collect system logs that indicate the status of the backup activities that help track the recovery plan progress.

Critical Cyber Assets Identification is a critical exercise of its own to identify and include all programmable electronic devices and communication networks including hardware, software, and data within the range of compliance to NERC CIP standards.

Overview of LogLogic® Compliance Suite: NERC Edition

The LogLogic Compliance Suite is a set of reports and alerts that are generated from logs from varied sources that are identified as Critical Assets under the NERC CIP guidance. The NERC Compliance Suite provides over 75 reports and 170 alerts to help:

- Establish a repeatable, faster compliance process to meet the NERC CIP requirements
- Provide the much needed information to map the technological controls to the regulatory standards, and
- Document the reports based evidence to control the costs of non-compliance risks and fines

The LogLogic Compliance Suite reports and alerts can be customized to extend to other compliance initiatives to improve the return on your investment in the LogLogic solutions. The compliance suites are built around a common security core to successfully implement security and compliance initiatives.

LogLogic Compliance Suite: NERC Edition - Sample Reports and Alerts

CIP-003-1	CyberSecurity – Security Management Controls	Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
Requirement	Description	Sample LogLogic Reports and Alerts
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 the Responsible Entity's needs and appropriate personnel roles and responsibilities.	<ul style="list-style-type: none"> Account activities on UNIX Servers Account activities on Windows Servers Accounts Added to Groups on Windows Servers Accounts Changed on UNIX Servers Accounts Created on UNIX Servers Accounts Removed from Groups on Windows Servers Accounts Locked Out of Windows Servers
CIP-005-1	CyberSecurity - Electronic Security Perimeter (ESP)	Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
Requirement	Description	Sample LogLogic Reports and Alerts
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.	<p>LogLogic solutions can assist in meeting R5 and R6 requirements of CIP-003:</p> <ul style="list-style-type: none"> Blocked URLs by Source Ips Allowed URLs by Source Users
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.	<ul style="list-style-type: none"> NERC: Cisco Switch Device Restart - Alert when a router or switch has been rebooted NERC: Disallowed Services - Disallowed firewall services NERC: NetApp Filer Unauthorized Mounting - Alert when someone unauthorized is trying to mount file system NERC: Windows Passwords Changed - Alert when users have changed their passwords NERC: Database Privilege Escalation - Alert when a connect to SYS or SYSTEM (or other - DBA accounts or roles) occurs from the command line or an application (stored procedures etc.)

More information

Visit www.loglogic.com or contact a LogLogic representative by e-mail: info@loglogic.com, or phone: 1.888.347.3883.