Federal Legislation Drives Historic Shift in Utility Industry Regulation

Bulk Power Suppliers Must Identify and Secure Telecommunication Vulnerabilities or Face NERC Fines of Up to $1 Million a Day

Overview

June 18, 2007 marked a historic transition in attempts to regulate the reliability of the U.S. electricity industry. As of this date, utilities and other bulk power providers were required to comply with mandatory and enforceable reliability standards for the first time in the industry's long history. These standards are developed and enforced by the North American Electric Reliability Corporation (NERC), which governs bulk power system providers and other industry members.

Though the U.S. electricity industry had long developed a host of operating guidelines, compliance was always voluntary. This changed with passage of the U.S. Energy Policy Act of 2005, whereby the U.S. Congress made NERC standards mandatory for all members of the bulk electricity industry.

Following this legislative action, NERC's Board of Trustees formally adopted a host of new *Reliability Standards* over the course of several meetings during 2006, and issued a calendar of effective dates for various provisions by which regulated managers of bulk electric systems must seek compliance.

Reliability Standards have been written and approved across fifteen categories, such as facilities design, emergency preparedness and operations, and personnel performance. Included is a host of standards for *Critical Infrastructure Protection* and *Communications*, which require strong measures to protect data and telecommunications network resources. These network security standards define obligations or requirements of utilities to ensure the reliable operation of bulk power systems by protecting, among other things, their Electronic Security Perimeter(s), Critical and Non-Critical Cyber Assets, and Telecommunication Systems. They are revised and updated regularly.

NERC is also responsible via federal legislation for regulatory compliance monitoring and enforcement, and has authority to levy substantial penalties for noncompliance. Under NERC's current enforcement structure, violation of any of these 83 standards will trigger punitive actions, including fines of up to $1 million a day.

After decades of voluntary compliance with guidelines issued from an industry-sponsored, self-policing organization, the U.S government now clearly requires that all bulk power suppliers make reasonable attempts to protect their data and telecom network resources from attack and disruption, or face stiff penalties and costly fines.

About NERC

The North American Electric Reliability Council became the North American Electric Reliability Corporation (NERC) on January 1, 2007. NERC was certified as the “electric reliability organization” by the Federal Energy Regulatory Commission (FERC) on July 20, 2006.

NERC provides the following definition of its mission, operational responsibilities, and legal authority:

> NERC’s mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Regulatory Commission to establish and enforce reliability standards for the bulk power system. NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the bulk power system; and educates trains, and certifies industry personnel. ERO activities in Canada related to the reliability of the bulk power system are recognized and overseen by the appropriate governmental authorities in that country. (source www.nerc.com)

NERC’s reconstitution as the electricity industry’s federally mandated regulatory organization has broad and substantial ramifications for North American power suppliers and the configuration and operations of their telecommunications facilities.

Telecom Security & Monitoring Solutions from SecureLogix

SecureLogix enables secure, optimized and efficiently managed enterprise voice networks. The company’s **ETM® (Enterprise Telephony Management) System** hosts a suite of integrated voice network security and management applications that protect critical network resources from telephony-based attack and abuse, and simplify voice network management. Together, these applications provide a powerful NERC compliance solution for bulk energy providers.

Central to the ETM System is the world’s first voice firewall and intrusion prevention system, dedicated to solving the unique security threats of real-time communications. These security solutions are integrated with powerful management capabilities to monitor voice network performance and audit service use and utilization.

Applications on customer voice-aware routers, COTS hardware, cloud servers, or SecureLogix Platform Appliances sit on the voice circuits between the PBX and the Central Office to monitor all inbound and outbound TDM and VoIP/SIP calls. Every inbound and outbound call is logged by the system, checked against voice network security access and usage policies, and monitored for call quality and performance.

The ETM platform hosts an integrated set of powerful applications including:

- *Voice Firewall* - The world’s only firewall for real-time media protects enterprise infrastructure by detecting and blocking TDM & VoIP attacks over voice lines, while controlling enterprise voice network access and service use.
- *Voice IPS* - Call pattern anomaly detection and prevention provides real-time detection of toll fraud, war dialing, service abuse/misuse for any type of voice network.
- *Usage Manager* - Enterprise-wide, IP-PBX / PBX-independent CDR collection, call accounting, resource utilization reporting, and traffic analysis providing granular and proactive voice network visibility to inform management decisions and provide full ROI.

- *Performance Manager* - A dashboard providing enterprise-wide visibility of both TDM and IP trunking infrastructure, with real-time and continuous monitoring of circuit health & status and call quality performance/QoS. Includes telecom error notification and threshold-based voice QoS alerting, with problem diagnosis and resolution tools.
- *Call Recorder* - Cost effective solution enables policy-based recording of targeted calls of interest.

SecureLogix Solutions are currently securing and managing over four million enterprise voice lines. The company's customers span nearly every industry vertical, from regional utilities, banks and hospitals, to the largest military installations and multi-national corporations.

NERC Requirements for Telecom Security & Monitoring

The following NERC standards and requirements address needs to ensure the reliability and security of bulk power systems by protecting critical assets and security perimeter(s) from unauthorized access and disruption over the telecom network.

Standard CIP-002-4a – Cyber Security – Critical Cyber Asset Identification	
Purpose	Provides a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
Requirement 2 – Critical Cyber Asset Identification	Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.
Relevance of Requirement(s) to Telecom Security	Voice lines are commonly used as authorized communication links to enable dial-up access to critical infrastructure systems (e.g. utility substation controls), as well as remote configuration and maintenance access for network resources (e.g. switches/routers, servers, firewalls). This requirement specifies that all resources that are accessible via dial-up modems are defined by NERC as "Critical Cyber Assets," and therefore are subject to reliability standards.
Compliance Solution	The SecureLogix ETM System is, by definition, a NERC Reliability Standards compliance solution. SecureLogix solutions are designed to monitor and protect key resources, such as those define by NERC as "Critical Cyber Assets," from unauthorized access and tampering via dial-up modem connections over voice lines.

Standard CIP-003-3 – Cyber Security – Security Management Controls	
Purpose	Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
Requirement 5 – Access Control	The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
Relevance of Requirement(s) to Telecom Security	NERC requires regulated entitles to manage lists of access privileges and related personnel for authorized dial-up modem access to Critical Assets.
Compliance Solution	The SecureLogix ETM System can maintain lists of authorized callers and associated firewall rules to allow and log authorized dial-up access to Critical Cyber Assets, while restricting access to all other inbound callers. ETM System access can be restricted to system administrators with associated privilege levels to write firewall rules and calibrate network access controls.

Standard CIP-005-3a – Cyber Security – Electronic Security Perimeter(s)	
Purpose	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 1 – Electronic Security Perimeter	The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
Requirement 2 – 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).
Requirement 3 – 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.
Requirement 4 – 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.
Requirement 5 – Documentation Review and Maintenance	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.

Relevance of Requirement(s) to Telecom Security	Today, attempts to identify and secure access points to an Electronic Security Perimeter often center on data network communication links to devices inside the perimeter. This singular focus overlooks one of the most traditional and widespread electronic access points: phone line, dial-up, modem connections into network resources. Unauthorized modem connections represent a significant security risk to any organization. Efforts to secure corporate networks begin by securing all connections to the Internet and other external public/private networks. Traditional data firewalls help monitor and secure corporate data connections. However, many organizations have not secured their telecom network, enabling employees to easily connect to the Internet over unmonitored corporate voice lines using personal modems and Internet Service Provider (ISP) accounts. Modems create direct, unsecured phone line access points into corporate data networks, opening the door for hackers, viruses, and other threats. Traditional data firewalls and PBX systems cannot see or stop modem calls and war-dialing attacks. War-dialing projects that scan for modems only provide a one-time, static snapshot of a very small portion of the unauthorized dial-up access points across the enterprise.
Compliance Solution	Unlike static war-dialers or modem scanners that find only a small subset of installed modems inside an organization, the SecureLogix ETM System uses patented technology to detect, alert, log, and filter all dial-up modem calls in real-time across the enterprise. The SecureLogix ETM System is the only technical means by which to fully identify, monitor, and control all unauthorized and authorized dial-up/modem access points into the Electronic Security Perimeter. The System's reporting engine provides complete voice network security logs and reports to satisfy record-keeping requirements.

Standard CIP-007-2a – Cyber Security – Systems Security Management	
Purpose	Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
Requirement 6 – 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.
Relevance of Requirement(s) to Telecom Security	The Responsible Entity must maintain logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
Compliance Solution	The SecureLogix ETM System monitors, detects, and logs all authorized and unauthorized modem calls across the enterprise. Alerts can speed incident response, and the System's reporting engine provides complete voice network security logs and reports to satisfy record-keeping requirements.

Standard CIP-008-3 – Cyber Security – Incident Reporting & Response Planning	
Purpose	The Responsible Entity must ensure the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets
Requirement 1 – Cyber Security Incident Response Plan	The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents.
Relevance of Requirement(s) to Telecom Security	Without real-time tools to detect and alert unauthorized network access via unsecured voice lines, many telecom-based security incidents are likely to go undetected and unreported.
Compliance Solution	SecureLogix solutions detect and log telecom-based security incidents, including modem activity, toll fraud, and unauthorized access to critical assets over the voice network.

Standard COM-001-1.1 – Telecommunications	
Purpose	Each Reliability Coordinator, Transmission Operator and Balancing Authority needs adequate and reliable telecommunications facilities internally and with others for the exchange of Interconnection and operating information necessary to maintain reliability.
Requirement 2	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications.
Relevance of Requirement(s) to Telecom Monitoring	Active management tools are needed to monitor the reliability and performance of vital communications facilities.
Compliance Solution	The ETM System's performance monitoring capabilities monitor the heath-and-status of voice trunking infrastructure, and can alert outages and error conditions that impact voice service reliability.

Summary

For the first time in the U.S electricity industry's long history, bulk power suppliers must comply with federally mandated requirements to monitor, manage, and secure their telecommunications networks, or face costly fines and other penalties. The ETM System from SecureLogix is a powerful compliance solution, satisfying many NERC reliability standards and requirements.

For more information, contact:
800-817-4837
www.securelogix.com

SecureLogix Corporation
13750 San Pedro, Ste. 820
San Antonio, Texas 78232