



Preparedness Protects Revenue

How Electric Utilities Can Comply with NERC CIP Reliability Standards and Maximize Network Availability





The electric power grid in North America is at risk, and the Federal Energy Regulatory Commission is taking action.

Comprised of legacy technologies now connected to wireless and IP-based networks, the electric power grid in North America provides an attractive vector for those with malicious intent to attack the systems that manage power in the U.S., Canada, and parts of Mexico. What was once closed, proprietary critical infrastructure can now potentially be accessed and compromised by anyone with some IT know-how, commonly available black hat-type tools, and a laptop.

Shield Your Networks from Growing Threat of Exploitation

Penetration tests have proved that an electric power network's critical components can easily be exploited by an unauthorized user via numerous points of entry on the Internet; a hacker can then sabotage the power supply to a particular region. The critical infrastructure networks that provide essential services to society are particularly susceptible to crippling attacks by criminal hackers or cyber terrorists. Jim Christy, Director of Future Exploration at the Department of Defense Cyber Crime Center, calls them "weapons of mass disruption."

Your networks become vulnerable as they can no longer be protected by traditional boundary defenses. An entirely redesigned network topology may be required for effective security and compliance with new North American Electric Reliability Corporation (NERC) standards for Critical Infrastructure Protection (CIP) aimed at reducing vulnerability. Today's "exposed" environment requires a re-architected set of scalable and auditable security policies and procedures to protect critical infrastructure, vital information flow and daily operations... in other words, your business.

Compliance Is Mandatory

In 2009, the Federal Energy Regulatory Commission (FERC) is expected to require North American electric utilities (there are more than 3,100 in the U.S. serving 131 million customers) generating or distributing power beyond a specified threshold to demonstrate 12 months of compliance with NERC CIP standards (www.ferc.gov/whats-new/comm-meet/072006/E-5.pdf). This means acceptable processes and practices must be in place by the end of 2008 in preparation for the following year's audits and full compliance, which is mandated by 2010.

Protect Your Business

What are the consequences of noncompliance? According to the FERC, utilities may face penalties of up to \$1 million a day per violation if they cannot show proof of compliance with NERC CIP standards (www.ferc.gov/whats-new/comm-meet/2007/101807/E-9.pdf). Currently, these are called "standards"; in 2009, they are expected to become federal law. Act now to reduce economic risk, human risk, legal liability risk and credibility risk. Protect your revenue stream.

Motorola: The Industry Leader in Security Services

A leader in wireless network technologies and security with more than 75 years of experience protecting mission-critical systems, Motorola continues to help critical infrastructure owners with the evolving security implications of convergent networks. Motorola Security Services:

- Understands the unique characteristics of SCADA, wireless and IT networks
- Applies proven operational expertise and discipline to critical infrastructure networks
- Brings the talent of engineers specifically certified to protect critical infrastructure
- Develops the reference architectures that secure networks and ensure regulatory compliance

Outsourcing security services enables you to focus on your business while Motorola focuses on security. Augmenting your security resources, Motorola helps you develop a cost-effective approach to compliance while maximizing network availability.

Motorola Security Services Delivers Customized Solutions

What are your primary concerns and top priorities? Whether you need a qualified resource to help with point solutions to ensure compliance, or a comprehensive and cohesive strategy that crosses organizational IT and Operations boundaries to prepare your company for current (NERC CIP) and future regulatory standards, Motorola can help. Covering the full gamut of physical and information security, the Motorola Security Services portfolio addresses the 2008 NERC CIP standards:

CIP Standards	Motorola Solutions
CIP-001: Sabotage Reporting	Policy Consulting
CIP-002: Critical Cyber Asset Identification	Security Assessments, Policy Consulting
CIP-003: Security Management Controls	Policy and Security Organization Consulting
CIP-004: Personnel & Training	Policy and Security Organization Consulting
CIP-005: Electronic Security Perimeter(s)	Assessments, Policy Consulting, Secure Design/Integration
CIP-006: Physical Security of Critical Cyber Assets	Assessments (Physical Security), Policy Consulting
CIP-007: Systems Security Management	Assessments, Policy Consulting, Secure Design/Integration, Security Monitoring (SOC)
CIP-008: Incident Reporting and Response Planning	Policy Consulting, Security Monitoring (SOC)
CIP-009: Recovery Plans for Critical Cyber Assets	Policy Consulting

Protecting SCADA Networks

Motorola also offers a **Critical Infrastructure Security Evaluation and Design Service** for Supervisory Control and Data Acquisition (SCADA) networks. Find out how effectively your core IT network and SCADA environment can defend against constantly evolving security threats. Motorola will assess your current vulnerability posture and make prioritized recommendations to help you achieve your security objectives.

Why We Must Act Now

An attack on the nation's electrical power infrastructure could require 12-18 months to replace critical components and restore activity, resulting in substantial economic loss and social impact. During the blackouts around the world in the summer of 2003, we learned that the consequences of even short-term power outages (hours) can be devastating.

Due to the potentially catastrophic consequences of a utility-based control system being breached, including compromised public safety and jeopardized national security, the government and industry called for mandatory security requirements, measured by audits, carrying stiff penalties for noncompliance. Hence, the new NERC CIP standards.

The time is now for a pragmatic security program that not only ensures compliance, but also maximizes network availability and protects your business.

For more information on how Motorola can help you architect and implement a security approach that minimizes cost and business disruption while ensuring NERC CIP compliance and protecting your assets, please contact Sam Cattle, Motorola Security Services Engagement Manager, 703-349-7171, or Sam.Cattle@motorola.com.

About Motorola Security Services

- Proven expertise in voice and data security for service providers, governments and enterprises
- Established track record of delivering design and implementation of complex infrastructure networks that are supported by a full range of professional and managed security services
- Holistic security framework that operationalizes security across the people, process, policy and technology foundations of each organization
- Practical hands-on experience with vulnerability assessment and mitigation, as they relate to threats associated with converged networks
- Onsite Security Assessments: Two-Way Radio Network, WLAN, WWAN, UMA, IMS, CDMA, GSM/GPRS, Wi4 WiMAX, UMTS, Physical and Facilities
- Defense-in-Depth Threat Management (Design, Managed Service, Integration) expertise
- Policy Design and Related Services (Incident Response Planning, Risk Management, Compliance)

About Motorola Services

Motorola Services, based on innovative technologies, delivers optimal solutions and managed services for service providers, governments and businesses. Motorola offers a comprehensive portfolio of cost-effective, high-performance services and applications that are robust and operational in critical multi-vendor, multi-technology environments. We leverage deep expertise in mobility, security and systems integration to deliver seamless communications. Motorola Services collaborates with customers to understand their needs and help them achieve their organizational objectives.



MOTOROLA

Motorola, Inc.
www.motorola.com

The information presented herein is to the best of our knowledge true and accurate. No warranty or guarantee expressed or implied is made regarding the capacity, performance or suitability of any product. MOTOROLA and the stylized M logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

© Motorola, Inc. 2007

1207NERCCIP