



GE MDS  
industrial wireless networks

WHITE PAPER

## GE MDS SOLUTIONS HELP ELECTRIC UTILITIES COMPLY WITH NERC/CIP SECURITY STANDARDS

With the power of the federal government behind it, the North American Electric Reliability Council (NERC) now has the legal authority to enforce reliability standards on all owners, operators, and users of the bulk power system, rather than relying on voluntary compliance.

In July 2006, the NERC's Critical Infrastructure Protection (CIP) standards went into effect with CIP compliance audits slated to begin in 2007. The question now facing utility organizations is, "are we ready?"

According to NERC, the intent of the CIP Cyber Security Standards is "to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems."

### **What can you do to comply?**

The standards outline specific requirements to protect access to communications devices and networks that use routable protocols, such as TCP/IP. When non-routable serial protocols, which are typically used in SCADA, are transported over IP—a common practice—they must then adhere to the same requirements of routable protocols.

There is an additional note of interest for utility companies not required to follow these new standards. According to a recent report completed by the Utilities Telecom Council (UTC), "...even if a utility does not fall under the standards, many other utilities are obliged to comply, and those companies will have to be comfortable with the security of their dealings with other utilities..."

UTC and other industry experts expect the standards eventually to have wider acceptance than NERC's current authority.

There are eight different CIP standards covering everything from Security Management Controls and Critical Cyber Assets, to Incident Reporting and Recovery Plans. Each one of the eight standards defines a series of specific requirements.

## CIP STANDARDS

Topic	New Standard Number
Critical Cyber Assets	CIP-002-1
Security Management Controls	CIP-003-1
Personnel and Training	CIP-004-1
Electronic Security	CIP-005-1
Physical Security	CIP-006-1
Systems Security Management	CIP-007-1
Incident Reporting and Response Planning	CIP-008-1
Recovery Plans	CIP-009-1



GE MDS radios help electric organizations meet several CIP standards as described in the table below. This table is organized by different CIP standards to demonstrate the features in specific radios that assist with each standard.

### CIP-004. PERSONNEL AND TRAINING

Requirement	Description	MDS Security Feature	MDS Product
CIP-004:R4.2	Revoke access of terminated personnel	RADIUS authentication allows for specific users to be removed from the list of allowed users	MDS iNET-II™, MDS iNET®, MDS Mercury™

### CIP-005. ELECTRONIC SECURITY PERIMETER

Requirement	Description	MDS Security Feature	MDS Product
CIP-005:R2.1	Explicit access must be specified	RADIUS authentication requires all users allowed to access the management interface to be defined	MDS iNET-II™, MDS iNET®, MDS Mercury™
CIP-005:R2.2	Enable only ports that are required	Enable/disable physical ports and Telnet/HTTP	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-005:R2.4	Ensure authenticity of accessing party	User authentication with RADIUS/CHAP on access to management interface	MDS iNET-II™, MDS iNET®, MDS Mercury™
CIP-005:R3.2	Detect and alert attempts or actual unauthorized access	SNMP traps sent on failed login attempts. Login sessions recorded in local event log file.	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-005:R4.2	Review of port settings	Retrievable configuration file allows off-line review of configuration. Remote management with Telnet/SSH allows real-time review of configuration parameters.	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-005:R5.1	Documentation that reflects current configuration	Retrievable configuration file aids in documenting configuration of radios	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™

## CIP-007. SYSTEMS SECURITY MANAGEMENT

Requirement	Description	MDS Security Feature	MDS Product
CIP-007:R2.1	Enable only ports and services that are required	Enable/disable physical ports and Telnet/HHTP	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-007:R2.2	Disable other ports and services	Enable/disable physical ports and Telnet/HHTP	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-007:R3.2	Document implementation of security patches	Current operating firmware in a radio is identified with a version number to help identify possible omissions in firmware upgrades	MDS iNET-II™, MDS iNET®, MDS entraNET™, MDS TransNET™, MDS 9710/4710
CIP-007:R5.1	Individual accounts and authorized access permissions	RADIUS authentication defines individual user accounts allowed to access the management interface	MDS iNET-II™, MDS iNET®, MDS Mercury™
CIP-007:R5.2.1	Removal of accounts or changing of password	RADIUS authentication helps to manage users allowed to access the management interface	MDS iNET-II™, MDS iNET®, MDS Mercury™
CIP-007:R5.3	Use of passwords	Required multi-character password	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-007:R6.2	Automated or manual alert of security incidents	SNMP traps sent out on events such as failed login attempts and successful logins, including the IP address of the user logging in	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-007:R6.3	Maintain a log of system events	Log file of events kept in non-volatile memory	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™
CIP-007:R7.1	Erase data storage to prevent unauthorized retrieval	Reset configuration settings to factory default	MDS iNET-II™, MDS iNET®, MDS Mercury™
CIP-007:R8.2	Cyber Vulnerability Assessment	Retrievable configuration file Display of current configuration	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™

## CIP-009. RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Requirement	Description	MDS Security Feature	MDS Product
CIP-009: R4	Backup and Restore	Loadable configuration files	MDS iNET-II™, MDS iNET®, MDS Mercury™, MDS entraNET™

There are several other ways that MDS radios can help meet NERC standards (CIP-006 Physical Security), however those measures require the installation of additional equipment external to the radio, for example video, where MDS radios provide sufficient speed to support the amount of data required to transmit video.

Readers interested in more information on industrial wireless solutions should contact GE MDS, 175 Science Parkway, Rochester, NY 14620, 585-242-9600. Additional information can also be found on the company's Web site at [www.gemds.com](http://www.gemds.com)

© 2007 GE MDS LLC Rev. 032307