



SecureWorks

Information Security Services

Achieving NERC CIP compliance with
Dell SecureWorks' Security Services



Introduction

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.” 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 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 CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system. After going into effect in June 2006, initial compliance auditing began in June 2007.

Dell SecureWorks has extensive experience partnering with utility providers and can help improve your security and compliance posture while reducing costs. As described below, many of our Managed Security Services and Security and Risk Consulting Services align directly with the NERC CIP Cyber Security Standards, allowing you to easily meet and exceed the requirements they set forth. Additionally, members of our Security and Risk Consulting team have deep expertise and extensive experience in NERC CIP compliance.

NERC CIP cyber security standards

NERC Category	Standard #	Requirement	Security and Risk Consulting	Managed Security Services
Auditing and Risk Assessment of Critical Assets	CIP-002	All network assets must be audited to identify Critical Cyber Assets. An Electronic Security Perimeter should be erected around these critical assets to provide protection. A risk-based assessment methodology should be utilized with annual reviews.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS
IT Policy Creation and Control	CIP-003	Policies with adherence monitoring and change control must be documented and in place.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Security Monitoring > SIM On-Demand
Change Control Management	CIP-003	Change Control policies and processes must be documented and adhered to.		
Critical Cyber Security Controls	CIP-003	Definitions and documentation on access control levels for critical assets such as Internet facing systems and critical backend solutions. Solutions should be in place to mitigate risks.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS > Security Monitoring > SIM On-Demand



NERC Category	Standard #	Requirement	Security and Risk Consulting	Managed Security Services
Security Awareness	CIP-004	Employees should be trained on policies, access controls and general awareness issues.	<ul style="list-style-type: none"> > Security Assessment > Security and Awareness Training 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS
Employee Background Checks	CIP-004	Background checks should be performed on all users with access to computer assets.	<ul style="list-style-type: none"> > CIP Gap Analysis 	
Electronic Security Protection	CIP-005	<p>An Electronic Security Perimeter should be established that provides the following:</p> <ul style="list-style-type: none"> • Disable Ports and Services that are not required • Monitor and Log Access 24x7x365 • Perform Annual Vulnerability Assessments (at a minimum) • Documentation of Network Changes 	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS > Security Monitoring > SIM On-Demand > Vulnerability Scanning
Physical Security Program	CIP-006	Physical Security controls should be documented and implemented that provide perimeter monitoring and logging, along with robust access controls. All cyber assets used for Physical Security are considered Critical and should be treated as such.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS > Security Monitoring > SIM On-Demand > Vulnerability Scanning
Systems Security Management	CIP-007	<p>All methods, processes and procedures for securing Critical Assets and all technology solutions should be well-defined and include automated controls. System and network events should be monitored automatically with alerts sent to key personnel.</p> <p>An annual vulnerability assessment should be performed.</p>	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS > Security Monitoring > SIM On-Demand > Vulnerability Scanning
Incident Response and Reporting	CIP-008	All cyber security incidents should be addressed by an internal computer incident response team (CIRT) and reported to the ES ISAC.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	<ul style="list-style-type: none"> > Managed Firewall > Managed NIPS/NIDS > Security Monitoring > SIM On-Demand > Vulnerability Scanning
Disaster Recovery	CIP-009	A disaster recovery plan should be created and tested with annual drills.	<ul style="list-style-type: none"> > Security Assessment > CIP Gap Analysis 	



SecureWorks

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

For more information, visit <http://www.secureworks.com>

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Availability varies by country. © 2011 Dell Inc. All rights reserved.

Dell and the Dell logo, SecureWorks, Counter Threat Unit (CTU), iSensor, iScanner, Sherlock, Inspector and LogVault are either registered trademarks or service marks, or other trademarks or service marks of Dell Inc. in the United States and in other countries. All other products and services mentioned are trademarks of their respective companies. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. February 2011.