Solution Overview: Symantec Managed Services

North American Electric Reliability Corporation (NERC) Cyber Security Standard

Symantec™ Managed Security Services Support for CIP Compliance

Overview

The North American Electric Reliability Corporation (NERC) is a not-for-profit corporation designed to improve the reliability and security of the bulk power system[1] in the United States, Canada and Northern Mexico. As the federally-designated Electric Reliability Organization (ERO) in North America, NERC develops and enforces mandatory standards that define requirements for reliable planning and operation of the bulk power system.

The Critical Infrastructure Protection (CIP) standard provides a cyber-security framework for the identification and protection of Critical Cyber Assets (i.e. devices that use a routable protocol or are dial-up accessible) that control or affect the reliability of North America's bulk power systems. In 2006, the U.S. Federal Energy Regulatory Commission (FERC)[2] made the CIP Cyber Security Standards mandatory for all Registered Entities identified by NERC, and enforceable across all users, owners, and operators of the bulk power system in the United States.

In the United States, NERC and its Regional Entities charged with compliance enforcement routinely monitor compliance. A number of methods, including regular and scheduled compliance audits, random spot checks, and any additional specific investigations as warranted, are used to identify where the standard may have been violated. Failure to comply can result in fines of up to $1 million per day, per incident, until a state of compliance is ultimately achieved.[3]

Symantec Managed Security Services Solutions for NERC CIP

Symantec Managed Security Services (MSS) delivers real-time threat monitoring and analysis to help utility providers demonstrate NERC CIP compliance to the appropriate Regional Entities of the NERC Compliance Audit Group. By partnering with Symantec MSS as their independent, remote security team, utility providers can leverage Symantec's global network of Security Operation Centers (SOCs), security experts, best practices, information correlation capabilities, and global intelligence to protect their Critical Cyber Assets.

Symantec MSS can help address these most pressing compliance and security needs:

- Protect against real-time threats in a fast-changing threat environment
- Improve the overall security posture to reduce the risk of compromise
- Gain control of security expenses with manageable, budgeted costs
- Eliminate the pressure and difficulty of finding, training, and retaining knowledgeable security personnel
- Demonstrate NERC CIP compliance with regulatory requirements to avoid potential penalties and increased regulatory scrutiny
- Lowers total cost of ownership by addressing multiple regulatory and compliance management and monitoring requirements, as well as internal policies

[1] NERC is responsible for aspects of an international electricity system that serves 334 million people, and has some 211,000 miles (340,000 km) of high-voltage transmission line. (http://www. nerc.com/page.php?cid=1|15)

[2] www.ferc.gov/media/news-releases/2006/2006-4/10-19-06-E-1.asp

[3] http://www.nerc.com/news_pr.php?npr=11; http://www.nerc.com/filez/enforcement/index.html

Providing effective security protection for utility providers requires powerful technology, accurate threat intelligence, proven processes, and experienced professionals. Symantec brings this altogether as an acknowledged industry leading Managed Security Service Provider (MSSP). Symantec maintains a 100% GCIA certification for analysts and the Security Operations Centers hold both the SAS70 Type II attestation and ISO27001 certification, which testify to our world-class service delivery.

The NERC CIP standard is a detailed, prescriptive approach for delivering a secure environment for the bulk power system. Symantec MSS addresses many of the defined CIP requirements. However, due to the complexities of the standard, additional security controls should be evaluated for full compliance. Symantec has an extensive security product and service portfolio, along with an extensive consulting and reseller partner network, to assist in meeting the requirements of NERC. The complete CIP standard can be downloaded from www.nerc.com under the “Standards/Reliability Standards” tab.

Meeting the Nine CIP Requirements

As a third-party monitoring entity with an independent perspective regarding NERC compliance, Symantec MSS enables organizations to meet the key Compliance Monitoring requirement found within each of the relevant CIP standards.

Utilities can offload the burden of real-time network monitoring to Symantec, while maintaining complete insight into their critical business information. Symantec MSS performs the critical tasks of log collection, management, advanced security analysis and global intelligence correlation to identify potential security threats that require immediate action, reducing the actions required by the utility’s IT security staff.

CIP-001 Sabotage Reporting

CIP-001 focuses on the reporting of physical assets rather than cyber security components of the bulk power system. Please consult the NERC CIP Reliability Standard for compliance requirements.

CIP-002 Critical Cyber Asset Identification

Symantec MSS supports the requirement to identify and protect Critical Cyber Assets of electric utility providers. During the MSS on-boarding process, Critical Cyber Assets are identified and related security protection infrastructure is monitored by Symantec MSS to ensure that the appropriate event logging is occurring.

Symantec MSS provides an organizational access model to support the requirement to recognize the differing roles of each entity in the operation of the bulk power system. In collaboration with the utility’s IT staff, Symantec MSS web portal access is structured to provide ‘need-to-know’ access to event logs and incident details based on the utility’s organizational structure. This ensures that access to security data is restricted to properly authorized security personnel.

MSS provides relevant security data to assist in the development of the annual compliance report. The secure web portal provides access to all security incidents and events that have been tracked throughout the year, with complete visibility to threat activity, trouble tickets and other notifications published. SOC clients also receive a monthly report that summarizes the analysis and actions taken, and participate in a periodic Service Review to discuss activity during the preceding period and pro-actively plan for the upcoming period.

- Symantec Managed Security Services: Security Monitoring Services

CIP-003 Security Management Controls

Symantec MSS uses consistent management procedures and best practices to protect information.

Symantec Managed Protection Services provide expertise to help secure and manage security architectures by remotely delivered change, lifecycle, and incident/fault management for network security infrastructure. Real-time monitoring of systems and applications ensures that proper security management controls are in place to make sure that Critical Cyber Assets are protected in support of CIP standards.

Symantec's SOC change management methodology is applied to all change requests for client devices. These procedures ensure that all changes are controlled, to include the submission, recording, approval, implementation, and post-implementation review.

As described above, MSS provides critical data to assist in the development of the annual compliance report via secure web portal, monthly reports and quarterly business reviews.

- Symantec Managed Security Services: Security Monitoring Services, Managed Protection Services

CIP-004 Personnel & Training

Symantec MSS provides ongoing security awareness through monthly security threat webcasts, ongoing notification of incident reporting, monthly incident activity reports and periodic service reviews. In addition, organizations can leverage Symantec Education Services, with access to an extensive professional training curriculum that covers security awareness, security policies and best practices.

- Symantec Managed Security Services: Security Monitoring Services

CIP-005 Electronic Security Perimeter(s)

Symantec Security Monitoring Services provide the operational foundation for the ongoing monitoring of the security perimeter (VPNs, modems and dial-up concentrators). MSS provides the secure management of these devices, delivering immediate notification of security incidents, policy exceptions, and access violations of monitored devices. In addition, MSS provides both reporting and evidentiary data to support audits, as well as support for the "Cyber Vulnerability Assessment" (defined in R4), with the ability of the SOC to verify the access controls on managed devices.

Symantec MSS security analysts use advanced tools and methodologies to monitor and analyze security log data on a 24x7 basis. Security incidents, ranging from routine network occurrences to actual attacks against an organization's systems, are identified through correlation and analysis of all monitored electronic access point-device logs such as firewalls, IDS/IPS, and VPN gateways. In addition, Symantec MSS analyzes device logs to detect patterns that indicate potential weaknesses or compromises in a utility's infrastructure.

The Vulnerability Management Service extends the Security Monitoring Service by identifying critical exposures in operating systems and applications across the organization. Data feeds from customer vulnerability scans are correlated with other MSS monitoring data to determine risk to either the Critical Cyber Asset or customer infrastructure. In addition, Symantec MSS is fully integrated with Symantec DeepSight Early Warning Services, and delivers customized alerts for new and existing vulnerabilities, as well as recommended countermeasures to prevent external attacks and internal sabotage before they occur.

MSS provides relevant data to assist in the development of the annual compliance report via secure web portal, monthly reports and periodic service reviews.

- Symantec Managed Security Services: Security Monitoring Services, Vulnerability Management Services, Symantec DeepSight Early Warning Services

CIP-006 Physical Security of Critical Cyber Assets

Symantec MSS provides a mature approach to physical security on a global basis, with strong security controls implemented at all SOCs. All Symantec best practices and methodologies have been audited against the ISO27001 criterion to protect Critical Cyber Assets monitored by Symantec MSS.

Symantec MSS meets the log retention requirement to assist in notification of security incidents to reporting authorities, clients or regulatory agencies. Authorized users have full access to all raw and correlated incident logs using immediately searchable online log data for 92 days. Raw logs are also stored off-line for one year as defined by NERC requirements. As needed, off-line storage can be extended in one-year increments to support exception retention requirements. All customers will have access to security incidents within the portal for the entire duration of their MSS contract to support investigative research or forensics analysis.

- Symantec Managed Security Services: Security Monitoring Services, Symantec DeepSight Early Warning Services

CIP-007 Systems Security Management

Symantec MSS implements consistent methodologies, processes, and procedures for securing Critical Cyber Assets within the Electronic Security Perimeter(s). Stringent test procedures are used to validate new functionality, enhancements and fixes to SOC infrastructure, as well as signatures, patches, configuration changes and other updates to client devices managed by MSS. All systems are thoroughly tested before deploying them into the production environment.

Centralized, automated security monitoring and analysis allow MSS security analysts to immediately detect and alert on suspicious activity, ensuring that only required ports and services are being utilized for authorized business traffic. MSS also tracks and monitors malicious activity by collecting logs from antivirus software and other security tools, as well as providing detection of connection attempts to botnet command and control servers.

By analyzing security incidents generated from log and vulnerability data, Symantec develops a deep understanding of the network environment, its vulnerabilities and threat activity, and uses this information to alert authorized security personnel to priority issues requiring attention.

- Symantec Managed Security Services: Security Monitoring Services, Managed Protection Services, Vulnerability Assessment Services, Symantec DeepSight Early Warning Services

CIP-008 Incident Reporting and Response Planning

Symantec MSS security experts follow best practices and standard procedures to ensure consistent service delivery, including; identification, classification, escalation, incident response, and reporting of security incidents as such events relate to Cyber Security Assets.

Through the secure web portal, authorized users can view the organization’s security posture and gain a deeper perspective on how to mitigate risks in the global threat landscape. Users can access at-a-glance summary pages, information on critical emerging threats and vulnerabilities, and recommendations on how to respond to security incidents and threats to an organization’s network. In addition, authorized Symantec DeepSight Early Warning Services users can conveniently access detailed research, in-depth analysis and expert guidance on mitigation strategies for up-to-the-minute information on the latest threats facing the utility’s network.

- Symantec Managed Security Services: Security Monitoring Services, Symantec DeepSight Early Warning Services

CIP-009-3 Recovery Plans for Critical Cyber Assets

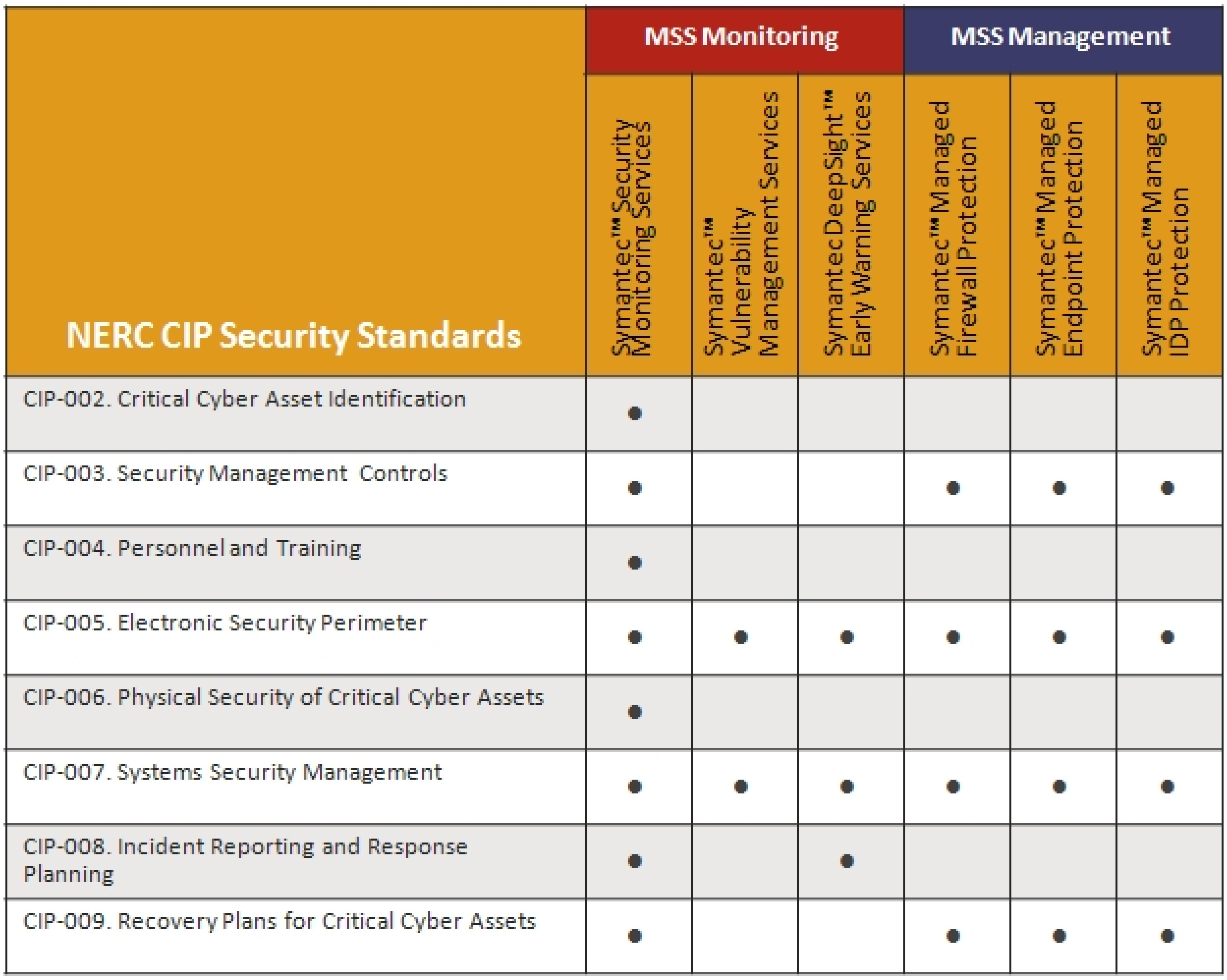
Symantec MSS provides a mature approach to business continuity and disaster recovery on a global basis, delivering built-in system redundancy to ensure that data is available when and where it is needed.

This includes failover to a U.S.-based data center, as well as across multiple SOCs worldwide. Symantec MSS best practices and methodologies are reviewed against ISO 27001 and SAS 70 Type II control objectives. In addition, each SOC maintains a well-documented Continuity of Operations Plan (COOP), including daily hand-off procedures used in our 24x7, “follow-the-sun” operations model.

For organizations that also contract for Managed Protection Services, device management includes a daily backup of device configuration. Since MSS has a full change history of every device in the ticket system, devices can be rolled-back into a previous configuration state if required.

- Symantec Managed Security Services: Security Monitoring Services, Managed Protection Services

Nine NERC CIP Requirements and Symantec Managed Security Services



	MSS Monitoring			MSS Management		
NERC CIP Security Standards	Symantec™ Security Monitoring Services	Symantec™ Vulnerability Management Services	Symantec DeepSight™ Early Warning Services	Symantec™ Managed Firewall Protection	Symantec™ Managed Endpoint Protection	Symantec™ Managed IDP Protection
CIP-002. Critical Cyber Asset Identification	●					
CIP-003. Security Management Controls	●			●	●	●
CIP-004. Personnel and Training	●					
CIP-005. Electronic Security Perimeter	●	●	●	●	●	●
CIP-006. Physical Security of Critical Cyber Assets	●					
CIP-007. Systems Security Management	●	●	●	●	●	●
CIP-008. Incident Reporting and Response Planning	●		●			
CIP-009. Recovery Plans for Critical Cyber Assets	●			●	●	●

Symantec Managed Security Services

Symantec MSS provides trusted solutions to identify and protect the Critical Cyber Assets used by utilities that provide services within North America's bulk power system. By partnering with Symantec MSS as their remote security team, organizations can leverage Symantec's global network of SOCs, security experts, best practices, correlation capabilities and intelligence to protect their IT assets, people and information in a rapidly evolving threat environment.

Complementary Symantec Products and Services

Symantec offers an extensive portfolio of security products and services to enhance security protection and address additional NERC requirements, including:

- Symantec Data Loss Protection – Simplifies the detection and protection of enterprise information
- Symantec Control Compliance Suite – Manage all aspects of IT risk and compliance at lower levels of cost and complexity
- Symantec Critical System Protection – Monitor and prevent malicious host activities to preserve system integrity and performance
- Symantec Protection Center – Unifies information security management across systems, networks and data to effectively protect against the inherent risks in today's IT infrastructures
- Security Advisory Services – Evaluates the maturity of a customer's information security program providing an understanding of anticipated exposure to information security risk likely to result from gaps within security programs
- Symantec Education – Extensive curriculum covering security awareness, security policies and best practices
- Symantec Security Information Manager – Enables a documented, repeatable process for security threat response and IT policy compliance via integrated log management and incident response solutions
- Symantec Endpoint Protection - Advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers in both physical and virtual environments
- Symantec NetBackup – Provides the ability to protect completely, store efficiently, recover anywhere, find easily and manage centrally

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com