



DATA SHEET



KEY BENEFITS

Rapid Compliance

There is no quicker way for public utilities to achieve compliance with NERC Cyber Security Standards, the Bioterrorism Act of 2002, SOX, or other regulations, or regulatory bodies such as the U.S. Health and Safety Commission (HSC).

Cost-Effective Solution

By leveraging VeriSign's expertise, resources, and economies of scale, utilities can reduce the costs of planning, developing, implementing, and managing the type of security infrastructure needed to achieve business objectives and comply with government regulations.

Flexible, Extensible Program

Utilities get a comprehensive solution that addresses current compliance issues, plus a framework of policies, procedures, guidelines, and technologies that can be adapted to new regulations and business priorities.

VeriSign® Security Services for Utilities

Public utilities are on the hot seat today, thanks in large part to the inexorable spread of Internet technologies. These critical-infrastructure custodians have become likely targets of cyber terrorism, and government regulations are requiring more vigilance. Historically, the distributed control systems (DCS), supervisory-control and data-acquisition (SCADA) systems, energy management systems, and distribution management systems that control utility plants and distribution grids were protected by proprietary technology and have been isolated from enterprise IT infrastructures. However, migration to standard operating systems, exposure of Internet connectivity, and requirements for remote access have opened these networks to the whole gamut of 21st-century cyber threats.

At the same time, utilities are under increasing pressure to comply with a growing body of industry and government regulations.

These regulations include:

- The North American Electric Reliability Council (NERC) Cyber Security Standards, commonly referred to as Critical Infrastructure Protection (CIP) standards 002 through 009, which require power utilities to assess and enhance their security environments
- The Homeland Security Act of 2002
- The Public Health Security and Bioterrorism Preparedness and Response Act (also called the Bioterrorism Act) of 2002, which required some water utilities to conduct a vulnerability assessment, develop an emergency response plan, and certify compliance by the middle of 2004

Other regulations also have an impact on the utility industry, such as the Sarbanes-Oxley Act (SOX), the California Security Breach Notice Act (formerly SB 1386) and other states' breach-reporting laws, and various federal Health and Safety Commission (HSC) regulations. Homeland security policies, focusing on cyber space as the next major terrorist battleground, are charging utility companies with protecting digital assets vital to national security while operating and maintaining networks that may become continually under attack. It is no small challenge to provide a high level of accessibility while minimizing risk.



+ The Bottom Line

VeriSign has a broad range of security services that help you achieve and maintain compliance with regulatory requirements and standards of good practice. In particular, our consulting services help you identify requirements and become compliant with key regulations and requirements such as NERC standards CIP-002 through CIP-009. In addition, a variety of managed services help you meet ongoing requirements more cost-effectively than implementing, operating, and maintaining such services yourself.

+ Enterprise Compliance Assessments

The VeriSign® Compliance Assessment and carries out these functions:

- **Identification of applicable security-related government and industry regulations** – VeriSign consultants help you assess compliance with applicable regulations, including NERC standards CIP-002 through CIP-009 for power companies, and the Bioterrorism Act of 2002, which is aimed at water utilities.
- **Organization of regulations into a requirements matrix** – VeriSign technologies and experts sift through often massive and complex government directives and reduce the information to specific security requirements that customers must meet.
- **Assessment of existing standard operating procedures (SOPs) against U.S. Department of Energy (DOE) regulations** – The DOE has delineated 21 steps for improving the cyber security of DCS networks, and VeriSign measures customer environments and practices against these guidelines. The DOE steps include proper backups and disaster-recovery plans, definition of security roles and responsibilities, training, configuration-management processes, intrusion detection, audits and surveys, and effective leadership.
- **Assessment against NERC standards CIP-002 through CIP-009** – NERC's mission is to ensure that the bulk electric system in North America is secure. The NERC regulations are similar to the DOE 21-step guidelines but more in depth, covering physical and electronic monitoring, test procedures, and appropriate responses to physical and electronic incidents.
- **Gap analysis and compilation of recommendations for remediation** – Regulatory requirements are viewed in the context of existing technologies and operational practices to see where the organization falls short of meeting identified requirements. These services include analysis of security policies, standard operating procedures (SOPs), systems and network architectures, and change-management procedures.
- **Management of remediation efforts** – VeriSign has vast experience providing support for program management in information-systems security; we have often assumed the role of interim (or deputy) chief information security officer (CISO). As such, VeriSign can be brought in to help manage remediation efforts required to quickly bring utilities companies into compliance.

+ Technical Security Assessments

NERC CIP-007 requires an annual cyber vulnerability assessment (which is good security practice in any case). VeriSign provides the following relevant services:

- **Architecture assessment** – Is your network secure and resilient? How are SCADA systems partitioned off from other less-safe zones? VeriSign operates its own critical infrastructure, and has extensive experience in helping companies redesign their networks to protect against attacks.
- **Network vulnerability assessments** – VeriSign performs technical testing and evaluation of your networks, devices, and servers—including DCS/SCADA systems and corporate infrastructure.
- **Application security assessments** – Although infrastructure is vital from the standpoint of availability and resiliency, business runs on applications. VeriSign helps you assess application security with a suite of consulting services that range from penetration testing to code review.

+ Program Development and Remediation

There is a lot of ground to cover in the NERC standards, not to mention requirements from other regulations and standards you may need to adhere to. VeriSign has significant experience in helping companies remediate audit findings and other types of weaknesses and vulnerabilities. Given our experience and knowledge base, we can help you resolve important issues more quickly than you could do yourself. Some examples include:

- **Program management** – VeriSign oversees remediation programs for you, prioritizing and managing key security improvement activities. In many cases, we have been appointed interim or deputy CISO for this sole purpose.
- **Policy development** – VeriSign has extensive experience in developing information security policies that meet regulatory and industry standards.
- **Incident response program development** – An incident response program is a key requirement of NERC CIP-008. VeriSign experts in incident management help you put together a comprehensive program to assess and respond to threats.
- **Business continuity and disaster recovery** – NERC CIP-009 requires mechanisms and processes for business continuity and disaster recovery. VeriSign experts help you perform business impact analyses and develop the appropriate recovery procedures.

+ Firewall Management

An electronic secure perimeter is a core requirement of NERC Cyber Security Standards. VeriSign® Firewall Management Service protects your critical cyber assets across networks, hosts, applications, and databases. VeriSign's highly trained security experts become an extension of your in-house IT staff, providing analysis, configuration, setup, alerts, and 24/7 system management. The customized firewall services harness industry best practices to help ensure a high level of network access and information availability, integrity, and privacy. VeriSign Firewall Management Service helps meet the monitoring and response requirements outlined in NERC standard CIP-005 by delivering around-the-clock firewall monitoring and generating immediate alerts and responses for service outages and security alerts associated with critical Internet access points.

+ Managed Intrusion Detection and Prevention

Monitoring electronic access is discussed in CIP-005 of the NERC Cyber Security Standards, and intrusion detection is also mentioned in the Systems Security Management requirements under CIP-007. VeriSign® Intrusion Detection Management Service (IDS) enhances an organization's network protection. To prevent costly downtime and potential loss of revenue, IDS provides a comprehensive, real-time warning system that proactively identifies and alerts against real security attacks. All intrusion attempts, regardless of severity, are logged, and well-defined customer notification and resolution procedures are executed for all security events.

The adoption of intrusion prevention technologies has created a unique challenge for security professionals. Creating and maintaining effective device policies requires extensive security expertise and time. If policies are incorrectly tuned to the customer's environment and not regularly updated, malicious traffic may be permitted and benign traffic may be blocked. In addition to managing intrusion prevention policies, security professionals must also monitor events generated from, and the health of, the devices on a continual basis. Device downtime can potentially result in either all traffic being blocked or malicious traffic being permitted into the company's environment. VeriSign® Intrusion Prevention Management Service (IPS) offers 24/7 management and monitoring of a wide range of technologies. Given our extensive security experience, intelligent infrastructure, and vendor-neutral support, VeriSign is in a unique position to deliver robust, customized management and monitoring solutions for intrusion prevention devices.

+ Vulnerability Management Services

The information protection and systems management requirements in CIP-007 of the NERC Cyber Security Standards address the inherent need to proactively identify and manage vulnerabilities across the network. VeriSign® Vulnerability Management Service provides the ideal solution for organizations seeking customized, cost-effective, and continuous protection against exploitable vulnerabilities. Its building blocks include an upfront risk assessment, recurring vulnerability scanning, vulnerability testing, and penetration testing. As an upgrade, VeriSign provides an alert service that correlates emerging threats against a host-based Vulnerability Management Service database that offers customers up-to-the-minute vulnerability intelligence.

+ Unified Authentication

Access control is addressed in NERC Cyber Security Standard CIP-005. This section requires that "the entity...implement strong procedural or technical controls to the access points to ensure authenticity of the accessing party." Strong, two-factor authentication provides a higher level of security than solutions based on static passwords alone. It helps prevent identity theft; allows you to open your network to partners, suppliers, and customers; and protects user devices and Web services. However, managing disparate, often-proprietary authentication mechanisms—digital certificates, dynamic one-time passwords (OTPs), and USB tokens—can be costly and complex. Besides eroding hardware and infrastructure budgets, proprietary or piecemeal authentication solutions can be difficult to integrate and often scale poorly, limiting your opportunities for expansion and collaboration.

VeriSign® Unified Authentication eliminates these constraints by providing a single, integrated platform for provisioning and managing all types of two-factor authentication credentials. VeriSign Unified Authentication reduces the cost of deployment by leveraging an enterprise's existing infrastructure, and it reduces the complexity of two-factor security and scalability. The combination of VeriSign's infrastructure, technology, data, and intelligence puts you in control of your security environment, leaving you free to focus on running and expanding your business.

+ VeriSign® Compliance Solutions

In addition to the regulations and standards that affect utilities companies, other regulations may apply as well. You may be subject to SOX and breach-reporting laws such as the California Security Breach Notice Act, or you may conduct commerce and fall under the Payment Card Industry (PCI) Data Security Standard. Regardless, VeriSign is your trusted security partner for a broad range of compliance needs. Our goal is to help you achieve and maintain compliance using the most cost-effective means possible. For more information about our full suite of compliance solutions, please visit our Web site at www.verisign.com.

+ The VeriSign Difference: Expertise, Intelligence, Trust

Few companies match VeriSign's experience and expertise, depth and breadth of services, robust infrastructure, intelligence, and role as trusted advisor. VeriSign® Security Services leverage exceptional knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and VeriSign's history of stability and trust to deliver cost-effective solutions for proactively managing information security risk.

The following characteristics distinguish and differentiate VeriSign offerings:

- **Global scale and intelligent infrastructure** – With a worldwide customer base and thousands of security devices under management, VeriSign has the scale to support the largest and most demanding organizations and the flexibility to support smaller enterprises where security is also a concern. The breadth of devices that VeriSign monitors affords the company a wider and deeper view of Internet activity. It leverages this unique threat intelligence, as well as the intelligence gathered by the VeriSign iDefense® Security Intelligence Services team to proactively identify—and alert customers to—emerging attack trends and cyber threats.
- **Seasoned practitioners** – With an average of more than ten years' experience in enterprise information security and three or more industry certifications per consultant, the VeriSign consulting team boasts one of the highest concentrations of credentialed experts in the industry. The security team's expertise, dedication, and focus on customer service help ensure that each customer not only gets a real-world solution that meets the unique requirements of its business, but also receives prompt attention when security events or other issues arise.
- **World-class support for industry-leading technology** – VeriSign delivers world-class services to enterprise customers by leveraging industry-leading technology; skilled experts; structured processes; and unique intelligence. As a services company, VeriSign focuses solely on designing and deploying security solutions that meet the specific requirements of its customers and maximize the effectiveness of their existing security investments.



DATA SHEET

- **Trusted partner** – VeriSign has a strong heritage in providing trusted security services, and thousands of organizations benefit from this heritage every day. Together with strong authentication, security consulting, threat intelligence, and e-commerce security, VeriSign® Managed Security Services represent an unparalleled commitment to helping enterprises engage confidently in electronic commerce, communications, and collaboration.

VeriSign is positioned in the Leaders Quadrant of the August 2007 “Magic Quadrant for MSSPs, North America, 1H07” Gartner report.

+ Learn More

For more information about VeriSign® Global Security Consulting or VeriSign Compliance Solutions, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

Visit us at www.Verisign.com for more information.

©2007 VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. The Magic Quadrant is copyrighted August 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

00017419 06-10-2006