



WHITE PAPER

Cybersecurity



Where it all comes together.™



CONTENTS

- + Executive Summary:
Forces of Change 3
- + Cyberspace and National Security 3
- + Cyberspace Security Requirments 4
 - Data Security 4
 - Continuity of Government 4
 - Interoperability 5
 - Regulatory Compliance 6
- + VeriSign Intelligence and
Control Services 6
 - Unique Data and Knowledge 6
 - Strong Authentication 6
 - Network Security 7
 - Application and Web-Services Security 8
 - Payment Services and
Transaction Security 8
- + Meeting Government
Cybersecurity Objectives 9
 - Ensure Continuity of
Government Services 9
 - Communicate and Collaborate Freely 9
 - Address Regulatory Compliance 10
 - Reduce Government Costs through
Public-Private Engagement 10



Executive Summary: Forces of Change

CYBERSPACE SECURITY PRIORITIES

The National Strategy to Secure Cyberspace identifies the following priorities:

- Create a national response system for cyberspace security that enables rapid information exchange and the resilience to restore full operations quickly (Continuity and contingency-plan development are also key objectives)
- Reduce threats and vulnerabilities, including improving infrastructure and technology and enhancing technological oversight
- Increase awareness of operational-security requirements, including implementation of multilevel certification programs for cybersecurity professionals
- Develop risk-management strategies, including risk assessment, prevention, transfer, and retention
- Secure government cyberspace to ensure delivery and continuity of essential government services (The ongoing E-Authentication initiative is a key component of this program, which offers the vision of a unified access and control system, accessible by all government agencies)

(Continued on next page.)

As the United States government moves forward with implementation of its new National Strategy to Secure Cyberspace, government agencies and private-sector enterprises are compelled to consider cyberspace, the Internet, and infrastructure security in a broader light. Until now, undertakings such as the Government Paperwork Elimination Act (GPEA) and business issues, such as regulatory compliance, risk management, and return on investment, have propelled the adoption of Internet and infrastructure security. Today, national security and the concomitant need to protect the nation's intelligent infrastructure and maintain the continuity of government and financial services are equally important drivers.

To proactively protect cyberspace, government agencies are focused on coordinating communications; securing transactions, email, and messaging; implementing reliable authentication and authorization mechanisms, and protecting critical information technology (IT) infrastructure. At the heart of these measures are digital-technology solutions that provide a trusted infrastructure.

VeriSign® Intelligence and ControlSM services combine VeriSign infrastructure, technology, data, and intelligence to deliver critical infrastructure services that make cyberspace more reliable and secure. Using VeriSign security services, government agencies can quickly deploy trusted infrastructure solutions that leverage existing investments to ensure the continuity of critical services and protect sensitive online documents, communications, and transactions.

Cyberspace and National Security

The strategic objectives of the National Strategy to Secure Cyberspace, as stated in its Executive Summary, are “to prevent cyber attacks against America's critical infrastructures, reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur.” The document acknowledges that the majority of the nation's intelligent infrastructure is run by the private sector, but it clearly recognizes that virtually every type of government service depends on cyberspace. “Governments at all levels perform essential services in the agriculture, food, water, public-health, emergency-services, defense, social-welfare, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping sectors that depend upon cyberspace for their delivery,” the document states.

Cyberspace security is crucial for maintaining the continuity of these vital services and for preserving the public's trust in information systems. It requires new levels of communication and cooperation, not only among government agencies and departments but also between government and the private sector. It involves protecting the nation's critical infrastructures from intrusion or attack as well as using the infrastructure as a tool with which law-enforcement, defense, and public-health agencies can gather, analyze, and disseminate information.

- Strengthen national security and international cooperation by improving counterintelligence, improving attack attribution and response, and expanding government-industry partnerships among international organizations to create watch-and-warning networks
- Use cybersecurity programs to protect privacy and civil liberties, thereby assuring consumers that their nonpublic information—for example, Social Security numbers, benefits information, and medical records—remains confidential
- Expand the Cyber Warning and Information Network in order to coordinate cyberspace crisis management (The network includes voice conferencing and data collaboration)
- Secure the Internet, including Internet protocols, physical devices, the domain name system, and the Border Gateway Protocol (used to interconnect the thousands of networks that make up the Internet)
- Foster trusted digital-control systems through the addition of security protocols and procedures
- Create secure wireless-communications networks
- Eliminate internal threats through implementation of operational-security procedures, including proper access control
- Continuously assess threats and vulnerabilities to federal cyber systems by creating a comprehensive, cross-government baseline of agency IT security performance

(Continued on next page.)

For optimal communication in cyberspace, the vast amounts of knowledge residing within each government agency must be linked. A strongly linked web of collaboration enables agencies to more quickly identify and isolate IT problems, such as viruses or other types of cyber attack. In terms of law enforcement, public safety, and national security, a linked infrastructure also enables the Internet to become a strategic vehicle for communication, especially in times of crisis.

An IT infrastructure with appropriate security controls is the first step in sharing information appropriately, efficiently, and promptly. Sound security policies and strong security mechanisms enable appropriate sharing of sensitive data, enabling government agencies to respond quickly, make well-informed decisions, and coordinate activities in the event of an emergency.

Cyberspace Security Requirements

To meet federal guidelines for protecting national security and to address internal business requirements for online security, cyber systems must be able to share data securely, ensure the continuous availability of critical services, interoperate across federal, state, and local systems, and comply with federal consumer-privacy regulations.

+ Data Security

As government agencies and departments open their networks and databases to share sensitive information with employees and partners in other agencies, the opportunities for unauthorized access, data tampering, and fraud increase. To safeguard mission-critical information and facilitate compliance with recent regulations regarding consumer privacy, data availability, and record keeping, government agencies must implement reliable mechanisms for user authentication, authorization, data privacy, and nonrepudiation. These mechanisms must protect not only human-initiated data exchanges but also machine-to-machine communications.

A reliable public-key infrastructure (PKI) is the first pillar of a trusted network, in which all people and all devices are strongly authenticated in an open, interoperable environment. In this environment, information can be securely shared and identities can be trusted across independent partners. The PKI enables information to be secured by digital-certificate-based services, including authentication, authorization, encryption, digital signing, and nonrepudiation.

+ Continuity of Government

Continuous availability of systems, services, and information is as important as protecting the privacy and integrity of data. Whether it's a natural disaster, such as a hurricane, or a disaster caused by terrorism, a hacker, or human error, government agencies face a variety of potential causes for disruption in operations. The quantitative losses associated with service disruption and system downtime can be expressed in terms of diminished productivity or lost revenues. However, the qualitative tolls related to service unavailability or impaired communications may ultimately present the greater risk to government agencies and the citizens they support. At their gravest, these costs could potentially be measured in lives lost or saved.

- Authenticate and maintain authorization procedures for users of federal systems to ensure that system users are who they say they are and are doing only what they are permitted to do
- Build the foundation for cybersecurity certification programs broadly accepted by public and private sectors
- Ensure that private-sector cybersecurity providers are certified as meeting certain minimum requirements

USING THE INTERNET FOR CROSS-AGENCY COMMUNICATION

Below are some of the current, innovative uses of Internet technology for communication and collaboration across government agencies:

- To catch known criminals—during, say, routine traffic stops or during fingerprinting at the time of arrest—records-management systems are being designed that offer real-time access to information contained in databases across state, local, and federal lines
- Public-health systems are being designed to analyze patterns of illness that show up in hospitals and other healthcare centers. Such patterning is essential in quickly recognizing and containing health threats that might otherwise go unnoticed

(Continued on next page.)

To maximize the availability and effectiveness of government services, agencies must maximize uptime and effectiveness of the security infrastructure. If the firewall itself is down, or if the intrusion-detection system (IDS) is not in operation, the entire network is open to security attacks. Uptime alone is not sufficient for network-security infrastructure; systems must also be effective. Networks need to be actively monitored and managed to prevent malicious attacks on the enterprise network and application infrastructure. According to the *Government Technology* magazine article “Tech Trends 2002,” researchers at MIT report, “The average machine is connected to the Internet for less than five minutes before an automated attack program scans it. . . . Once a system is compromised, it can be used as a jumping-off point for deeper attacks, as into [government] infrastructure and connected systems.”

In considering continuity of services, agencies must also attend to the DNS infrastructure. Preventing a single point of failure caused by an attack on the DNS infrastructure has been largely overlooked as a critical component of network continuity. However, when the DNS server goes down, enterprise Web sites and email services are inaccessible, and online transactions and communications cannot be conducted—an unacceptable condition in handling emergencies or conducting business in real time.

To ensure that critical services are not disrupted and to enable rapid identification of and response to system attacks, government agencies must develop and implement business-continuity plans for all major aspects of IT infrastructure, including applications, data storage, facilities, and networks. They must protect the core infrastructure of the IT system, including the servers, routers, and other components that move traffic back and forth. Systems must be able to quickly and reliably detect intrusions and protect against denial-of-service attacks and other assaults. In addition, they must be engineered to scale during a crisis and must have built-in redundancies so that services and information are available even if one part of a network, system, or infrastructure fails.

+ Interoperability

Underscoring the need for business continuity and improved communication and collaboration is the need for a secure, standards-based IT infrastructure. Without a common set of standards, data sharing can be difficult, ineffective, and costly. To ensure that important data is available to all authorized users, government and private-sector agencies must adopt and enforce open IT standards across federal, state, and local agencies. By implementing a flexible, standards-based infrastructure that allows disparate systems to securely communicate with one another, government agencies can cost-effectively share information with all authorized users.

Standardization must also be addressed at the level of data-organization. Though data-warehousing and business-intelligence systems have made inroads into information access and analysis, regardless of platform or database, the lack of a common standard has often hampered success. Daily business processes generate vast amounts of information; all of which is stored throughout government departments in a variety of legacy, client/server, and standalone workstation databases.

- New Global Information System (GIS) interoperability allows federal, state, and local agencies to share location-based information. Fire, police, public-works, public-health, building and safety, water, engineering, utilities, and other departments are expanding use of GIS to plan appropriate responses to public emergencies and protect high-risk facilities
- Scientists are developing border-information systems that act on preset triggers. For example, when a person or item crosses a given border, an information profile is generated. This profile enables enforcement agents to take appropriate action
- Customer-relationship-management (CRM) centers are being created to field and route huge volumes of calls during an emergency, using virtual private networks (VPNs) and secure government land and satellite lines. These CRM centers will also be able to field calls from the public, such as those reporting health emergencies, handling requests directly or routing them to the appropriate agency

+ Regulatory Compliance

Though not a direct requirement of the new cybersecurity strategy, regulatory compliance is a key issue whenever data is shared online. As government agencies open their networks to share information with other agencies and with the private sector, compliance with new consumer-privacy regulations becomes part of any cyberspace initiative. To ensure compliance, agency managers must establish administrative, technological, and physical safeguards to protect the confidentiality and integrity of customer records, ensure the 24/7 availability of specific information, and enable auditing.

VeriSign[®] Intelligence and ControlSM Services

As the leading provider of intelligent infrastructure services, VeriSign helps government agencies address the issues of data security, business continuity, and interoperability. Intelligence and Control services combine agencies' unique data and knowledge about security patterns and trends with its technology and infrastructure to deliver strong-authentication, network-security, application-security, and payment services. Using these services to protect critical data and assess, monitor, manage, and respond to security threats and vulnerabilities, government agencies can communicate and collaborate freely with other agencies, ensure continuity of services, address regulatory-compliance issues, and conduct commerce more securely.

+ Unique Data and Knowledge

VeriSign operates a majority of the intelligent infrastructure that supports the Internet, resolving more than 14 billion DNS lookups and 400 million intelligent database lookups daily, handling 2.7 billion Signaling System 7 (SS7) messages every day through its telephone network, securing more than 400,000 Web sites worldwide, and processing more than 35 percent of e-commerce transactions in North America through its payment gateway. Processing such high-transaction volume affords VeriSign a unique look into data and knowledgebase related to Internet security and provides in-depth visibility into global security and fraud trends. VeriSign offers a unique integration of infrastructure, best-of-breed technology, data insight, event correlation and analysis, contingency planning, and overall security intelligence to provide unmatched control of each security environment, leaving agencies free to concentrate on core business.

+ Strong Authentication

To securely collaborate with colleagues, ensure business continuity, and comply with government regulations, government agencies must be able to authenticate and authorize internal and external users and reliably secure online data exchanges, transactions, and communications. VeriSign security services help protect data from end to end. Using the proven VeriSign[®] Managed PKI, government agencies can deploy a full range of authentication solutions for all users and all devices.

PKI TERMINOLOGY

The following terms are frequently used when referring to the services provided by a public key infrastructure (PKI).

- **Authentication** determines which employees, partners, devices, and other system users can access the system, and verifies their identity when they attempt to access the system. Authentication also verifies the identity of applications and sites providing services.
- **Authorization** (also called access control) determines which information or resources a user can access and which operations it can perform once it gains access to the resource.
- **Encryption** encodes documents and transactions to protect the confidentiality of data as it travels across the network, and allows only the intended recipient to decode a document.
- **Digital signing** provides the electronic equivalent of a handwritten signature. Digital signatures are used to create an algorithm (hash) that mathematically represents the exact structure and composition of a given piece of data. This electronic footprint enables agencies to verify the integrity of the data and determine whether it has been tampered with in transit.
- **Nonrepudiation** helps prove the state of data at a given time as well as its origin and reception; it is used for auditing, accountability, and fraud prevention.

(Continued on next page.)

VeriSign Strong Authentication includes digital-certificate-based authentication, encryption, and nonrepudiation services for users and devices; two-factor authentication—combining a digital certificate with a smart card, universal serial bus (USB) token, or biometrics provided by a VeriSign partner—and server and device certification. Leveraging the highly scalable Managed PKI, government agencies can cost-effectively establish a robust, customized PKI and certificate-authority (CA) system for issuing digital certificates throughout their IT enterprise.

Managed PKI is designed to secure intranet, extranet, and Internet applications while enabling fluid interaction with partners, mobile workers, Web-services devices, and other users. In addition, the service can be seamlessly integrated with leading access-control applications such as IBM® Tivoli® Access Manager™ to provide granular role- and user-based access control.

+ Network Security

To ensure the continuity of government services, government agencies must not only protect the network infrastructure from attack or accidental failure, but also implement mechanisms to ensure service availability in the event one part of the system does go down. VeriSign® Global Security Consulting, VeriSign® DNS Assurance service, and VeriSign® Managed Security Services (MSS) help ensure that the network infrastructure operates effectively 24/7 by enabling government agencies to optimize network processes as well as assess, prevent, and respond to system attacks and failures.

VeriSign® Global Security Consulting

Identifying network vulnerabilities, assessing potential risks, and evaluating the effectiveness of current safeguards is a complex task that requires in-depth knowledge of security technology and practices, as well as continual identification of ever changing security threats and requirements. VeriSign leverages deep expertise, proven methodologies, and state-of-the-art assessment tools to thoroughly evaluate the vulnerability of existing network-security implementations including policies, technology, operations, use, performance, and physical security.

The VeriSign consulting team identifies immediate security concerns and pinpoints gaps between the current infrastructure and identified requirements for overall system security and projected growth. Using this information, it provides prioritized recommendations for improving performance and mitigating risk while maximizing the value of existing investments.

VeriSign subject-matter experts also work with the agency's internal security team to design, develop, and implement a customized risk-management program that cost-effectively addresses key gaps in security. Services may include preparing a comprehensive security-policy document, providing for protection and monitoring of network solutions, developing auditing and reporting methodologies for proving regulatory compliance, optimizing network performance, reliability, and scalability, and creating disaster-recovery and business-continuity plans to ensure high availability. By drawing on the skills and expertise of the VeriSign team to ensure that network-security operations are reliable, scalable, and secure, government agencies help protect critical infrastructure and ensure continuity of services.

VeriSign® DNS Assurance Services

VeriSign DNS Assurance services enable government agencies to ensure continuous availability of Web sites, Web services, and email services by eliminating single points of failure in their DNS infrastructure. As the operator of the world's largest DNS infrastructure,

VeriSign: PARTNERING WITH GOVERNMENT

The VeriSign global infrastructure plays an integral role in national cybersecurity, and its contributions to government cybersecurity range from managing critical infrastructure to helping develop open standards. The following list identifies some of the areas in which VeriSign contributes to government cybersecurity.

- Manages a key portion of the Internet's intelligent infrastructure and provides core security services to enterprises, government, and the public
- Runs two network-operating centers which, according to the federal government, are classified as national IT assets
- Manages two of the nation's 13 Internet A-root domain name system (DNS) servers
- Helped shape U.S. Department of Homeland Security (DHS) guidelines through consultation with security experts from the DHS, the National Security Council, the Office of Homeland Security, the Department of Commerce (DOC), and the U.S. National Security Council (NSC)
- Plays an active role in key critical-infrastructure policy groups, including:
 - +The U.S. National Security Telecommunications Advisory Committee (NSTAC), an advisory group of CEOs to the president

(Continued on next page.)

VeriSign leverages its multiple global server locations to build redundancy in and provide service-level agreements (SLAs) of 100 percent uptime for DNS resolution, ensuring that critical government services can be accessed 24/7. Government agencies can offload management of the secondary DNS server or both the primary and secondary DNS servers to VeriSign. In either case, DNS Assurance services are delivered via the proven, global infrastructure that VeriSign operates, guaranteeing unmatched reliability and scalability.

The VeriSign® MSS Suite

The VeriSign MSS suite of services maximizes both uptime and effectiveness by enabling government agencies to offload security and infrastructure management to a team of experts whose core business is security. The components of the suite, which can be utilized individually or as a set, include assessment, monitoring, management, incident response, and reporting. Working from VeriSign globally linked network-operation centers, security teams use sophisticated tools to monitor, correlate, and analyze data across multiple levels of the organization in order to rapidly identify and prevent attacks. Agencies maintain full control of security policies and decisions and can access network data 24/7 via a Web-based customer portal. Industry-leading SLAs help agencies avoid the financial risks inherent in system downtime. The MSS suite includes managed firewall, IDS, VPN, and two-factor authentication services, as well as service from the VeriSign technical help desk.

+ Application and Web-Services Security

The security requirements that apply to data exchanges between people also apply to automated data sharing among applications. To connect internal applications to partner and supplier applications, government agencies must ensure that machine-to-machine communications can reliably secure data, validate the identity of applications, check the data integrity, and log and archive system activity.

VeriSign services for assessing, managing, and monitoring Web-service security enable government agencies to extend application-integration initiatives to partners, colleagues, and suppliers with confidence that valuable data is protected from end to end. Using a unique Web-services methodology—including Web-strategy assessment and planning, Web-security design and architecture, Web-security integration, and Web management and monitoring, VeriSign offers a cross-platform, standards-based security solution for making applications available for use over the Internet.

VeriSign® Application Security Services use agency-defined criteria to establish secure connections between business partners and back-end applications, authenticate an application's credentials in real time, authorize access to specific applications, apply and verify digital signatures, encrypt and decrypt application requests and responses, and monitor and log system activities. Using VeriSign application services, agencies can securely access applications across legacy and nonlegacy systems, increasing agency efficiency and improving service.

+ Payment Services and Transaction Security

To prevent fraud, ensure prompt delivery of services, and facilitate regulatory compliance, government agencies need a secure, reliable, and scalable system for processing online payments. VeriSign is the Internet's largest provider of trusted payment processing, and more than 94,000 customers use VeriSign payment services. These services give e-government managers a simple, unified method for processing online payments and interacting with banks and institutions that process credit cards and debit cards.

- +The U.S. Federal Communications Commission's Network Reliability and Interoperability Council (NRIC), which addresses cybersecurity, law enforcement, network reliability, and physical-security infrastructure
- +The NSC, as a core adviser on Internet-service provider/Internet security work being done by the president's Cyber Security Board
- +The Information Security (InfoSec) Committee of the Information Technology Association of America, an influential Washington, DC, organization that develops recommendations for information-security and infrastructure-protection program recommendations
- +The Partnership for Critical Infrastructure Security, consisting of members from the White House, the NSC, the Commerce, Justice, Energy, and Defense departments, and the business community (rail, telecommunications, finance, IT, and energy)
- +The Computer Emergency Response Team (CERT), a federally funded group out of Carnegie-Mellon University, in Pittsburgh, Pennsylvania, that shares information on cybersecurity activity; the Internet Security Alliance arm of CERT provides information on overcoming disruptions of service to businesses

(Continued on next page.)

VeriSign payment services replace time-intensive point-to-point processing with a secure Internet gateway that supports multiple platforms and payment types, connects to leading payment processors, and is packaged for easy integration into Web-application environments and back-office systems. The robust, paperless e-business system can time stamp and store for auditing as many as 500,000 transactions per day. It also includes fraud filters and IP-address monitoring to further reduce the risk of fraud. Using VeriSign payment services, agencies can buy and sell products securely over online channels, thereby reducing costs, improving services, and enabling compliance with government regulations.

Meeting Government Cybersecurity Objectives

The highly reliable and scalable constellation of VeriSign security services helps government agencies meet cybersecurity objectives by ensuring continuity of critical services, enabling secure communication and collaboration, supporting regulatory compliance, and creating a public to private architecture that alleviates the burden of building and maintaining an internal security solution.

+ Ensure Continuity of Government Services

VeriSign helps government agencies ensure network-infrastructure availability and continuity of government services through its DNS Assurance, MSS, and Global Security Consulting services. By managing critical parts of an agency's network infrastructure, VeriSign ensures 24/7 availability of an enterprise's network architecture, and thereby, continuous delivery of critical services. To ensure that agencies can always communicate and collaborate securely, the highly scalable and robust VeriSign Managed PKI is also designed to ensure continuity of government services.

The VeriSign security infrastructure is based on disaster-hardened facilities, U.S. Department of Defense-grade physical security, biometrics, intrusion detection, and stringent computer-data and network-security measures to ensure that root keys are not compromised and that PKI service is never disrupted.

+ Communicate and Collaborate Freely

Unfettered data sharing, communication, and collaboration requires not only reliable security mechanisms but also easy interoperability with applications and devices, regardless of platform or environment. VeriSign security services help government agencies meet both requirements. VeriSign authentication, application-security, and payment services provide a high level of trust among online partners, helping government agencies to collaborate and communicate more efficiently and securely. To enable interoperability with virtually any device, anywhere, anytime, VeriSign services are built on open standards to ensure maximum flexibility.

The VeriSign Managed PKI, for example, enables interoperability with virtually any application or device and is preintegrated with leading off-the-shelf solutions, including Microsoft applications, Microsoft® Windows® operating systems, and IBM® Lotus Notes®, as well as Nortel Networks™, Cisco®, and Check Point products. The VeriSign Trust

- +The Information Technology Information Sharing and Analysis Center (IT-ISAC), an infrastructure organization focused on sharing information on hacks and other threats between its members and government agencies
- +The Organization of Economic Cooperation and Development (OECD), a global organization that regularly advises on security practices
- Utilizes SSL certificates to provide information security for more than 400,000 Web sites
- Secures 35 percent of e-commerce transactions in North America through its payment gateway

MANAGED PKI CHECKLIST

VeriSign Managed PKI services strengthen cybersecurity by giving government agencies the following capabilities:

- Control access to intranets and extranets
- Authenticate senders and recipients in e-commerce transactions and email exchanges
- Provide confidentiality and data integrity for email and Internet exchanges
- Authenticate and encrypt data exchanged between Web services
- Implement VPNs using the Internet Protocol Security (IPSec) protocol for confidentiality and data integrity

(Continued on next page.)

Gateway supports open standards for Web services, including Simple Object Access Protocol (SOAP), Extensible Markup Language (XML) Signature, XML Encryption, XML Key Management Specification (XKMS), Direct Internet Message Encapsulation (DIME), and Web Services Security (WS-Security) specifications.

+ Address Regulatory Compliance

The comprehensive enterprise security services that VeriSign provides help government agencies address current regulatory-compliance issues while building a framework for adapting to new government regulations. VeriSign regulatory-compliance solutions enable government agencies to address the following federal regulations.

- **California SB 1386:** This bill requires any agency, business, or person owning, licensing, or maintaining a computerized database of personal information on California residents to immediately notify California residents if the security of their personal information is compromised. This requirement, which became operative in July 2003, is likely to be duplicated by other states and applies even if no information is stolen. In addition, it authorizes lawsuits and injunctions if breaches are not reported in a timely manner.
- **21 CFR Part 11:** Pharmaceutical companies, medical-device manufacturers, and government agencies are increasingly using the Internet to automate business processes, such as clinical trials, drug-research collaboration, and drug approvals. As a result, there is renewed interest in compliance with the U.S. Food and Drug Administration's (FDA) 21 CFR Part 11 regulation for electronic records and electronic signatures, which addresses risk assessment and management, system monitoring, access control, authentication, encryption, and digital-signature requirements.
- **The Gramm-Leach-Bliley Act (GLBA):** Also known as the Financial Modernization Act, the GLBA requires banks, insurance companies, brokerages, and other financial institutions to establish administrative, technological, and physical safeguards to ensure the confidentiality and integrity of customer records and information. To comply with this federal mandate, financial institutions are required to identify and assess security risks, plan and implement security solutions to protect sensitive information, and establish measures to monitor and manage security systems.
- **The Health Insurance Portability and Accountability Act (HIPAA):** As healthcare agencies move information online to automate business processes, streamline communications, and improve customer service, safeguarding electronic data has evolved from an internally defined business practice to an externally imposed requirement of the federal government. HIPAA requires health plans, clearinghouses, healthcare providers, Medicare/Medicaid agencies, and other healthcare organizations to comply with strict regulations regarding the confidentiality, integrity, and availability of private health information.

+ Reduce Government Costs through Public-Private Engagement

Because a successful security solution requires state-of-the-art technology, sophisticated certificate practices, and highly trained personnel, internal deployment of PKI and other security services involves significant investments of time and money. In an internal deployment, the agency assumes 100 percent of the responsibility for provisioning, deploying, and maintaining the security infrastructure and services, as well as all the surrounding technology. The agency is also responsible for providing a secure facility, which must have physical site security, Internet-safe network configurations, redundant systems, disaster

- Attach digital signatures to electronic forms
- Address compliance issues related to the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill (SB) 1386, the Gramm-Leach-Bliley Act (GLBA), and the U.S. Food and Drug Administration's 21 CFR Part 11 regulation
- Easily administer server certificates, enabling agencies to authenticate servers and Web sites to visitors and to encrypt Web transactions and communications
- Cost-effectively establish a robust PKI and CA system while alleviating the risks and burdens of internal PKI deployment, maintenance, and oversight

recovery, viable PKI legal practices, financially sound liability protection, and highly trained personnel. If any of these components is weak, the agency may be compromised. Finally, the process of planning, purchasing, implementing, deploying, and testing internal security services can take many months, delaying the deployment of cybersecurity initiatives and leaving agency services vulnerable to disruption.

By outsourcing PKI and network security to VeriSign, government agencies alleviate the burdens and risks of building, deploying, and maintaining internal security services, while maintaining control over vital aspects of security such as security policy, authentication models, and certificate-lifecycle management. Agencies can leverage industry-leading technology from VeriSign, as well as the company's expertise and industry-standard certificate-practices statement to not only reduce costs, speed time to deployment, and strengthen security but also to free resources to focus on their core missions.

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