



INTERNET
SECURITY
SYSTEMS™

How To Take The Fear Out Of Bringing Government Systems Online

November 2001

Introduction

Most government agencies recognize increasing demands for online government services, both from constituents and from other governmental entities. They genuinely want to provide self-directed customer service, Web-based transactions, online information resources and streamlined communication channels. Adding to the pressure, the Government Paperwork Elimination Act (GPEA) mandates that by October 2003, transactions with the federal government must be available online unless there's a compelling reason to maintain a primarily paper-based system. Clearly, government agencies recognize that online systems:

- Deliver services directly to constituents at lower cost with greater flexibility than traditional delivery mechanisms
- Reduce operational expenses, especially with limited staff and budgets.
- Deliver a tangible return on investment
- Improve operational efficiencies
- Streamline the flow of information between governmental entities, and between agencies, businesses and taxpayers

This last point is particularly crucial. The recent terrorist actions highlight the liabilities of unlinked government information systems, and emphasize the need for better coordination in the future. Previously isolated databases must talk to each other in the future if homeland security and similar initiatives that cut across traditional local, state and federal boundaries are to have any reasonable expectation of success.

So, Why The Hesitation?

Despite a good understanding of the compelling reasons to make transaction, commerce, information and communications processes available online, government organizations have been significantly slower than the private sector in adopting Internet and other networking resources. There are several valid reasons for these delays.

Fear of Losing the Public Trust. Government agencies understand the importance and sensitivity of the information they collect. If any income, social security numbers, or other key identifiers and information were to become public, the repercussions in terms of loss of goodwill and potential criminal liability would be severe. And government databases carry tremendous amounts of information that would be of great value in the wrong hands – everything from personal identification resources to classified documents and archives. Even without criminal intent, the need to preserve the public trust is of paramount concern. Public trust in the government's ability to safeguard their information could be compromised, or even destroyed.

Anxiety Over National Security. In the wake of September 11, concerns about online attack and misuse, including espionage, have made it clear that a concerted attack on Internet-based technologies can create a sense of panic similar to what anthrax scares have done to the U.S. Postal system – even when those attacks are unsuccessful. On a pragmatic level, many governmental entities feel that it's better to err on the side of caution. In other words, no information access is better than access that places anything at risk. Even though the private sector and the military have long track records of successful information security practices, risk adverse managers will often use security as an excuse to avoid innovation.

Concern over Potential Internal Abuse. While many government employees at a variety of different levels have always had access to sensitive information, having that information online presents new opportunities for misuse. Imagine the havoc that a disgruntled government employee could wreak on an organization by quietly deleting critical information – or publishing sensitive data on a Web site. Without a full understanding of how to supervise and enforce access to online information, agency managers will be wary of introducing additional levels of technology and transparency into their daily operations.

Inadequate In-House Skills and Knowledge. Most government agencies recognize the basic need for secure, online information services. What they often lack are employees who understand the technological intricacies of online information protection. So, they may latch onto buzz-products that sound like they'll protect information systems, or may begin a deployment, only to back off once the scope of the commitment is fully understood. The relative scarcity of security expertise and high salaries this staff commands only complicates the equation.

Limited budgets and staff resources. Protection for online resources is not a core competency for most governmental entities. As a result, it is difficult for agencies to establish a clear, tangible benefit for information protection expenditures. With inadequate funding and already overburdened staff, good security practices are difficult to establish and enforce.

While each rationale has validity, these reasons for not speeding the development of secure online information systems may soon be irrelevant. Directives set in Washington are expected to force information protection compliance on even smaller governments or agencies. Standards such as ISO 17799 (a ten-part, widely recognized security process standard), and legislation like the Gramm-Leach-Bailey Act and HIPAA are first steps towards what promises to be increasing attention to the flow of information through and across departmental lines, and out to the general population.

In particular, the newly created Office of Homeland Security regards information protection as a key component of its mission. As Richard Clarke, the national advisor on cyber-security, pointed out to an audience of security experts, privacy advocates and policy-makers, "Our information infrastructure is fragile because we didn't build it to do the things that it is doing. That has to change."¹ The question for any governmental entity, therefore, is if it will be ready once these new standards have been set.

The Basics of Government-Based Online Information Protection

Fortunately, federal, state and local governments have established models to use as they build appropriate online information security strategies. Many agencies already deliver key services online, including license renewals, check distribution, payroll processing, and much more. These operations already operate securely, with careful attention to people, processes and technology that:

Assures Availability – Systems must be up when needed. If they aren't, people will stop trying to use them. More importantly, people will associate "not there when I need it" with the agency in general.

Ensures Integrity – Constituents must feel secure that no one can tamper with their online transactions, and that databases are accurate and reliable. No one wants to find out that they're on the FBI's "most wanted" list as part of a prank, and no one wants to discover that nuclear munitions listed as secured are, in fact, missing. In other words, data that isn't reliable is often much worse than no data at all.

Protects Privacy – If constituents believe that private data might be openly available to others, they will urgently avoid using any systems that might make their information openly available. Since human nature tends to distrust technology when it comes to privacy, even the slightest appearance of a lapse may be enough to deter widespread acceptance of any online initiative.

In addition to the basic needs detailed above, information sharing programs that address national security and other cross-jurisdictional concerns must also:

¹ Lemos, Robert, "Net Threat: Enemies At The Gate," ZDNet News, November 8, 2001.

Anticipate System Attacks/Misuse by obtaining current online attack trend information from reliable sources. Any trusted relationship is only as strong as its weakest link. Agencies must be sure their partners are properly anticipating and responding to threats.

Securely share information with security providers and law enforcement agencies. Failure to share information and coordinate response hampers the global threat recognition necessary to deter coordinated attacks. However, this information itself must be carefully protected from attack and misuse as it moves across multiple jurisdictional boundaries.

Protect shared security information resources, including both public and private threat recognition and response centers, security information databases and research facilities. Since ownership of many of these resources will be shared jointly among multiple participants, it is critical that secure operations be established from the outset, with clearly delineated responsibilities for all participants.

A Secure Information Protection Platform

There are two basic components in an effective information protection strategy – technology and expertise. These elements apply equally to in house or managed security solutions.

A **pervasive protection platform** provides comprehensive, flexible and adaptive protection across networks, servers and desktops. In other words, it continuously assesses vulnerabilities and identifies active threats, no matter where an online risk exposure may appear. It must bring a wide range of security technologies – active blocking, malicious code control (active content and/or antivirus), PKI, VPN, vulnerability assessment, policy distribution and enforcement, IDS, application protection, and security decision support – into an easy to use, centrally managed framework so that it addresses specific organizational needs and operational IT functions.

Internet Security Systems' protection system for networks, servers and desktops, is an excellent example of such a platform. This powerful family of sensors with centralized configuration, management and reporting services can be flexibly deployed in any number, placement or combination to provide comprehensive coverage – including remote desktops and wireless installations.

The benefits of this architectural approach are immediate and obvious. The platform can be deployed in a simple configuration to begin with, then more comprehensively as a return on investment is realized. Centralized configuration and management mean security operations – including incident management, policy distribution and reporting – can be fully integrated throughout the organization. Since each protection system's configuration and reporting console is designed for a specific subset of the overall information protection process, the time needed to deploy an information protection solution and the training needed to manage it is significantly compressed. Automated policy distribution and audit capabilities carry the bulk of day-to-day security operations, so the government agency can focus on the actual services and transactions it delivers. As a result, significantly less time and expense are spent on security management and more resources are available for other tasks.

The Expertise: Continuous Research, Analyses, Education and Improvement

Technology is only half the battle. Vulnerabilities, threats and response procedures evolve rapidly and continually. Therefore, the second half of an effective, cost-effective information protection solution requires **knowledge, experience and expertise** in order for the technological solution to be effective. Without proactive research into new threats and attack trend analysis, ongoing education and proper security procedures, any security solution will be unnecessarily obtrusive towards normal operations at best, and increasingly ineffective as time goes by.

If an agency has the size, budget and compelling need for an in-house solution, its leaders must seek a vendor with experience in the governmental arena who can deliver a complete solution – assessment, design, deployment, management, support and education. For example, Internet

Security Systems has established the **X-Force™** organization, a unique branch of its knowledge services dedicated to threat intelligence collection, attack trend, tracking and public dissemination of critical security information, as well as product-oriented research and development. This forward-thinking combination of integrated services is unprecedented in the industry and can position an agency's internal staff stay on top of security issues as they evolve.

Many government organizations do not have the budget or need for an in house security solution. In such cases, a managed solution may be a better value. With a managed solution, the agency works with an established vendor with government experience, such as EZGov. EZGov is a government information systems specialist whose proprietary software solutions link governments with their constituents. Or they might contract for online security from a telephony or Internet services provider, like BellSouth.

The benefits of an appropriately designed managed security solution can be significant. A good managed solution offers a single point of contact for a variety of security needs. Since security hardware, software and staff are employed by the solution vendor, agencies save on staffing, hardware and software expenses. Operational security costs become fixed items with predictable cost, and may easier to approve, especially if the security services provider is already approved as an authorized vendor of other services.

Best of all, managed solutions put the onus of remaining up to date firmly on the service provider. Since these agents concentrate solely on security, they see a wider variety of threats have a deeper investment in staying abreast of breaking trends and have deeper experience in emergency response than all but a few non-specialists can possibly match.

As in all technology purchases, those in charge of establishing and securing government systems should be sure to aggressively research the company's track record with respect to systems security. Check the company's references. Review case studies thoroughly. Look for best-of-breed technology, experienced consultants and an established methodology for addressing today's – and tomorrow's – evolving government systems security needs.

Conclusion: Proper Security Practices Position Agencies to Thrive Online

The demand to bring government services and transactional applications online is growing daily. However, the issues that hinder the progress of such initiatives are valid, and have caused many organizations to delay their online initiatives. Fortunately, there are successful, proven models for how to move government services online. Whether in house or through a managed solution, this process need not be excessively costly, nor should it be disruptive to normal operations. The key is proper selection of an information security vendor, so that the availability, integrity and privacy of information can be reasonably ensured. As government agencies move ahead to deliver online services their various constituencies, these integrated, well-designed security systems will deliver the security assurances government agencies need to move online with confidence.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect critical online resources from attack and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East.

Copyright © 2001 - 2002, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo and X-Force are trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.