Priority IV: Securing Governments' Cyberspace

Although most critical infrastructures are in the private sector, governments at various levels perform many key functions. Among those key functions are national defense, homeland security, emergency response, taxation, payments to citizens, central bank activities, criminal justice, and public health. All of those functions and others now depend upon information networks and systems. Thus, it is the duty of governments to secure their information systems in order to provide essential services. At the federal level it is also required by law.

The foundation for the federal government's cybersecurity requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable for fulfilling those responsibilities, and integrating security requirements into budget and capital planning processes.

The federal government will lead by example, giving cybersecurity appropriate attention and care, and encouraging others to do so. The federal government's procurement practices will be used to help promote cybersecurity. For example, federal agencies should become early adopters of new, more secure systems and protocols where appropriate.

State and local governments can have a similar effect on cybersecurity. The federal government is ready to partner with both state and local governments to promote cybersecurity.

Within the federal government the Director of OMB is responsible for ensuring that department and agency heads carry out their legal responsibilities to secure IT systems, with the exception of classified systems of national security departments and agencies that are the responsibility of the Secretary of Defense and the Director of Central Intelligence.

A. THE FEDERAL GOVERNMENT

Beginning with the Budget Blueprint in February 2001, continuing in the fiscal year 2002 and 2003 budgets, and the Management Reform Agenda, this administration has set a clear agenda for government reform. These reforms include unifying federal government security and critical infrastructure protection initiatives, and making strong security a condition of funding for all federal investments in information-technology systems.

The *National Strategy to Secure Cyberspace* supports these efforts by working to ensure that the federal government can identify vulnerabilities, anticipate threats, mitigate attacks when possible, and provide for continuity of operations.

To overcome deficiencies in cybersecurity, OMB established a governmentwide IT security program, as required by law, to set IT security policies and perform oversight of federal agency compliance with security requirements. This program is based on a cost-effective, risk-based approach. Agencies must ensure that security is integrated within every IT investment. This approach is designed to enable federal government business operations, not to unnecessarily impede those functions.

1. Continuously Assess Threats and Vulnerabilities to Federal Cyber Systems

A key step to ensuring the security of federal information technology is to understand the current state of the effectiveness of security and privacy controls in individual systems. Once identified, it is equally important to maintain that understanding through a continuing cycle of risk assessment. This approach is reflected in OMB security policies, and is featured in FISMA.

OMB's first report to Congress on government information security reform in February 2002 identified six common governmentwide security performance gaps.

These weaknesses included:

(1) Lack of senior management attention;

(2) Lack of performance measurement;

(3) Poor security education and awareness;

(4) Failure to fully fund and integrate security into capital planning and investment control;

(5) Failure to ensure that contractor services are adequately secure; and

(6) Failure to detect, report, and share information on vulnerabilities.

These gaps are not new or surprising. OMB, along with the General Accounting Office and agency inspectors general, has found them to be problems for at least 6 years. The evaluation and reporting requirements established by law have given OMB and federal agencies an opportunity to develop a comprehensive, cross-government baseline of agency IT security performance that had not been previously available. More importantly, through the development and use of corrective action plans, the federal government has a uniform process to track progress in fixing those weaknesses.

Before OMB approves funding for a system an agency must demonstrate that it has resolved outstanding security issues related to the system. Additionally, agencies must ensure that security has been incorporated and security costs reported for every IT investment through the federal capital planning process. OMB policy stipulates that specific lifecycle security costs be identified, built into, and funded as part of each system investment. Failure to do so results in disapproval of funding for the entire system.

2. Agency-Specific Processes

The federal government must have a comprehensive and crosscutting approach to improving cybersecurity. Three processes central to improving and maintaining federal cybersecurity in the agencies are: identifying and documenting enterprise architectures; continuously assessing threats and vulnerabilities, and understanding the risks they pose to agency operations and assets; and implementing security controls and remediation efforts to reduce and manage those risks. Each agency will be expected to create and implement this formal three-step process to achieve greater security.

a. Identify and Document Enterprise Architectures

OMB policy requires each agency to identify and document their enterprise architecture, including an authoritative inventory of all operations and assets, all agency IT systems, critical business processes, and their interrelationships with other organizations. This process yields a governmentwide view of critical security needs.

Through the budget process, the federal government will drive agency investments in commercially available tools to improve their architectures and system configuration. Configuration management and control has incidental and important benefits to security. For example, controlling system configuration permits agencies to more effectively and efficiently enforce policies and permissions and more easily install antivirus definitions and other software updates and patches across an entire system or network.

b. Continuously Assess Threats and Vulnerabilities

Commercially available automated auditing and reporting mechanisms should be used to validate the effectiveness of the security controls across a system and are essential to continuously understand risks to those systems. These tools can help in analyzing data, providing forward-looking assessments, and alerting agencies of unacceptable risks to their operations.

Federal agencies will continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and actively deploy threat management tools to deter attacks. The federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools. (A/R 4-1)

c. Implement Security Controls and Remediation Efforts

The implementation of security controls that maintain risk at an acceptable level can often be accomplished in a relatively brief amount of time. However, the remediation of vulnerabilities is a much more complex challenge. Software is constantly changing and each new upgrade can introduce new vulnerabilities. As a result, vulnerabilities must be assessed continuously. Remediation often involves “patching” or installing pieces of software or code that are used to update the main program. The remediation of federal systems must be planned in a consistent fashion.

B. ADDITIONAL GOVERNMENTWIDE CHALLENGES

In addition, there are four specific governmentwide security challenges that need to be addressed. Each agency, as appropriate, should work with OMB to resolve these challenges.

1. Authenticate and Maintain Authorization for Users of Federal Systems

Identifying and authenticating each system user is the first link in the system security chain, and it must take place whenever system access is initiated. To establish and maintain secure system operations, organizations must ensure that the people on the system are who they say they are and are doing only what they are authorized to do. Many authentication procedures used today are inadequate. Passwords are not being changed from the system default, are often incorrectly configured, and are rarely updated.

The federal government will continue to promote a continuing chain of security for all federal employees and processes, including the use, where appropriate, of biometric smart cards for access to buildings and computers, and authentication from the moment of computer log on. The benefits of such an approach are clear. By promoting multi-layered identification and authentication—the use of strong passwords, smart tokens, and biometrics - the federal government will eliminate many significant security problems that it has today.

Through the ongoing E-Authentication initiative, the federal government will review the need for stronger access control and authentication; explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms; and consequently, further promote consistency and interoperability. (A/R 4-2)

The National Information Assurance Partnership (NIAP)

NIAP is a U.S. Government initiative to meet testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the Computer Security Act of 1987.

The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the Nation's critical information infrastructure. More information on the partnership can be found at http://www.niap.nist.gov.

2. Secure Federal Wireless Local Area Networks

When using wireless technology, the federal government will carefully evaluate the risks associated with using such technology for critical functions. The National Institute of Standards and Technology (NIST) notes that wireless communications can be intercepted and that wireless networks can also experience denial-of-service attacks. Federal agencies should use the NIST findings and recommendations on wireless systems as a guide to the operation of wireless networks.

Federal agencies should consider installing systems that continuously check for unauthorized connections to their networks. Agency policy and procedures should reflect careful consideration of additional risk reduction measures, including the use of strong encryption, bi-directional authentication, shielding standards and other technical security considerations, configuration management, intrusion detection, incident handling, and computer security awareness and training programs. (A/R 4-3)

3. Improve Security in Government Outsourcing and Procurement

Through a joint effort of OMB's Office of Federal Procurement Policy, the Federal Acquisition Regulations Council, and the Executive Branch Information Systems Security Committee, the federal government is identifying ways to improve security in agency contracts and evaluating the overall federal procurement process as it relates to security. Agencies' maintenance of security for outsourced operations was cited as one of the key weaknesses identified in OMB's February 2002 security report to Congress.

Additionally, the federal government will be conducting a comprehensive review of the National Information Assurance Partnership (NIAP), to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of products reviewed under the NIAP or similar evaluation processes. (A/R 4-4)

Department of Defense (DOD) policy stipulates that if an evaluated product of the type being sought is available for use, then the DOD component must procure the evaluated product. If no evaluated product is currently available, the component must require prospective vendors to submit their product for evaluation to be further considered.

Following this program review, the government will evaluate the cost effectiveness of expanding the program to cover all federal agencies. If this proves workable, it could both improve government security and leverage the government's significant purchasing power to influence the market and begin to improve the security of all consumer information technology products.

4. Develop Specific Criteria for Independent Security Reviews and Reviewers and Certification

With the growing emphasis on security comes the corresponding need for expert independent verification and validation of agency security programs and practices. FISMA and OMB's implementing guidance require that agencies' program officials and CIOs review at least annually the status of their programs. Few agencies have available personnel resources to conduct such reviews, and thus they frequently contract for such services. Agencies and OMB have found that contractor security expertise varies widely from the truly expert to less than acceptable. Moreover, many independent verification and validation contractors are also in the business of providing security program implementation services; thus, their program reviews may be biased toward their preferred way of implementing security.

The federal government will explore whether private sector security service providers to the federal government should be certified as meeting certain minimum capabilities, including the extent to which they are adequately independent. (A/R 4-5)

C. STATE AND LOCAL GOVERNMENTS

American democracy is rooted in the precepts of federalism—a system of government in which power is allocated between federal and state governments. This structure of overlapping federal, state, and local governance has more than 87,000 different jurisdictions and provides unique opportunity and challenges for cyberspace security efforts. State and local governments, like the federal government, operate large, interconnected information systems upon which critical government services depend.

States provide services that make up the “public safety net” for millions of Americans and their families. Services include essential social support activities as well as critical public safety functions, such as law enforcement and emergency response services. States also own and operate critical infrastructure systems, such as electric power and transmission, transportation, and water systems. They play a catalytic role in bringing together the different stakeholders that deliver critical services within their state to prepare for, respond to, manage, and recover from a crisis. Delivering critical services unique to their roles and responsibilities within our federalist system makes state government a critical infrastructure sector in its own right.

Many of these critical functions carried out by states are inexorably tied to IT—including making payments to welfare recipients, supporting law enforcement with electronic access to criminal records, and operating state-owned utility and transportation services. Preventing cyber attacks and responding quickly when they do occur, ensures that these 24/7 systems remain available and in place to provide important services that the public needs and expects. Information technology systems have the potential for bringing unprecedented efficiency and responsiveness from state governments for their residents. Citizen confidence in the integrity of these systems and the data collected and maintained by them is essential for expanded use and capture of these potential benefits.

With an increasing dependence on integrated systems, state, local, and federal agencies have to collectively combat cyber attacks. Sharing information to protect systems is an important foundation for ensuring government continuity. States have adopted several mechanisms to facilitate the sharing of information on cyber attacks and in reporting incidents.

These mechanisms are continually modified and improved as new policy emerges and as technological solutions become available. In addition, states are exploring options for improving information sharing both internally and externally. These options include enacting legislation that provides additional funding and training for cybersecurity and forming partnerships across state, local, and federal governments to manage cyber threats.

1. DHS will Work with State and Local Governments and Encourage them to Consider Establishing IT Security Programs and to Participate in ISACs with Similar Governments

State and local governments are encouraged to establish IT security programs for their departments and agencies, including awareness, audits, and standards; and to participate in the established ISACs with similar governments. (A/R 4-6)