

STATEMENT OF
THE HON. MARK A. FORMAN
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES
June 24, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the positive actions being taken by the federal government to address IT security challenges and issues. As noted in OMB's May 16th Report to Congress on Federal Government Information Security Reform, progress was made in FY 2002 to identify and begin to address long-standing IT security problems that are both serious and pervasive. This trend has continued in FY 2003 with Departments and agencies further strengthening management, operational and technical controls. Much work remains, however, for security to be adequately incorporated into the life-cycle of all IT investments. OMB intends to lead this effort through coordinated management and budget processes.

Measuring Agency Performance

Annual IT security reviews

In accordance with the Federal Information Security Management Act (FISMA), agency Chief Information Officers (CIOs) and program officials must conduct annual IT security reviews of their programs and the systems that support their programs. Additionally, agency Inspectors General (IGs) are asked to perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews and evaluations are reported annually to OMB.

FY 2001 reports, conducted pursuant to the Government Information Security Reform Act (GISRA), established a baseline of agency IT security status. To ensure that progress could be consistently determined against that baseline, OMB's FY 2002 reporting instructions remained nearly identical to the FY 2001 requirements. The FY 2002 reporting instructions also included common IT security performance measures. For the first time, using these performance measures, the Federal government is able to determine progress in IT security. Federal agencies, OMB, the Congress, and the General Accounting Office are able to track and monitor agency status and progress using those measures.

OMB Analysis of Agency Reports

As stated in my April testimony, agencies have demonstrated quantifiable progress in conducting activities such as risk assessment, security planning, certification and accreditation and contingency planning. From FY 2001 to FY 2002, the Federal government made progress across all areas of IT security performance measures. Sixty-five percentage of federal systems in FY 2002 had been assessed for risk, 62% had an up to date security plan, 47% had been certified and accredited, and 55% had a contingency plan. The Clinger-Cohen report included in the President's 2004 budget builds on this pattern of improvement and establishes a goal that 80% of Federal IT systems be certified and accredited by the end of December 2003.

Additionally, agencies have reported that, in accordance with FISMA requirements, they are testing an increasing percentage of their systems for weaknesses in management, operational and technical controls.

At many agencies, program officials, CIOs, and IGs are engaged and working together. IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process. Some IGs and CIOs, however, have significantly different views of the state of the agency's security programs. Agency heads need to understand the reason for such differences where they exist.

FISMA legislation requires that federal agencies report any significant deficiency in a policy, procedure, or practice as a material weakness. Over half of the large agencies (14 out of 24) have declared at least one material weakness relating to IT security. Deficiencies are noted in a number of areas including access controls, configuration management, risk management, security policy, physical security, intrusion detection, incident handling, training, and testing of contingency plans. Through the Plan of Action and Milestones (POA&Ms) process, OMB will oversee work by federal agencies to close these material weaknesses and substantially decrease the number that are repeated from prior fiscal years.

Increasing Agency Attention to IT Security Remediation

OMB has found that agency senior managers are paying greater attention to IT security. In accordance with OMB guidance, CIOs and program officials must maintain POA&Ms to ensure that program and system level IT security weaknesses are tracked and corrected. The agencies include in their plans the name of the person responsible for correcting the weakness, the resources required and the target completion date. Agencies provide quarterly updates to OMB on their progress in remediating their IT security weaknesses. To assist agencies and OMB in better tracking progress, agencies will also include with their quarterly updates their status against the IT security performance measures in OMB guidance. These updates will help inform the quarterly assessment of the President's Management Agenda scorecard.

Ensuring Effective and Accountable Information Security

While awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. Increased understanding of IT security requirements along with improved accountability will assist program officials in successfully securing their programs and services.

Rather to appropriately secure our operations and assets, all Federal employees must recognize and fully meet their security roles. Those agency officials with additional responsibilities, such as agency program officials and the agency CIO must be held accountable for meeting those responsibilities. The owner of a system must ensure that security has been incorporated throughout the entire life-cycle of the system, from planning and developing through operations and maintenance. Increased understanding of IT security requirements along with improved accountability will assist program officials in successfully securing their programs and services. OMB will continue to reinforce the responsibilities of agency program officials and CIOs via management and budget processes.

Additionally, OMB is working with federal agencies to ensure that CIOs have the necessary authority to ensure effective information security throughout the agency. This authority includes:

- Establishing and enforcing department-wide information system security policies, protocols and procedures;
- Approving IT investments, including proposed investments in information security;
- Managing the activities of component (e.g., bureau) CIOs;
- Regularly monitoring the security of all department systems and networks;
- Establishing and routinely updating department business continuity plans;
- Ensuring appropriate information security staffing and ongoing commitment to training throughout the department; and
- Ensuring the appropriate level of security awareness, including adherence to policies, protocols and procedures, throughout the department.

In FY 2002, OMB found that more Departments are exercising greater oversight over their bureaus. Additionally, nearly all agencies have designated a senior information security officer.

Improving Security Education and Awareness

Through the Administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were made available to all Federal agencies in late 2002. Initial courses were targeted to CIOs and program managers with additional courses to be added for IT security managers, and the general workforce. Agencies have also conducted on-site information security training sessions for their employees.

OMB Guidance on the Federal Information Security Management Act

GISRA, as well as its successor, FISMA, have both been instrumental in improving the state of Federal IT security. The framework and processes in law and OMB policy have underlined the importance of management, implementation, evaluation, and remediation to achieving real IT security progress.

OMB guidance to agencies and IGs on reporting the results of annual security reviews is largely consistent with the previous year's GISRA guidance. The guidance highlights the differences between GISRA and FISMA and reinforces the need for accountability through performance measures. The guidance also targets IG actions to assess agency remediation efforts. Accordingly, each IG will assess the existence of a Department-wide remediation process.

Integrating Security into Capital Planning and Investment Control

OMB continues to actively work with federal agencies to ensure they incorporate security into the capital planning and investment control process. The FY 2004 President's Budget established the goal that by the end of 2003, 80% of the Federal government's FY 2004 major IT investments will appropriately integrate security into the lifecycle of the investment.

Agencies have been instructed to report on their compliance with security requirements, i.e. development of security plans and certification and accreditation activities, when requesting funds for major systems. Failure to appropriately incorporate security in new and existing IT investments automatically requires the business case to be scored as "at-risk". As a result, that system is not approved for the fiscal year in which the funds were requested until the security weaknesses are addressed. There are approximately 495 systems in the FY 2004 budget at-risk either solely or in part due to IT security weaknesses. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems that possess out-of-date certification and accreditation.

Many agencies are not adequately prioritizing their IT investments and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

Spending on IT security continues to increase. For FY 2002, Federal agencies spent about \$2.7 billion from a total IT investment of about \$48 billion. OMB estimates FY 2003 funding for IT security investments of \$4.2 billion, and in FY 2004, Federal agencies plan to spend over \$4.7 billion on IT security. Based on IT spending data and agency IT security performance, spending more on IT security does not always improve IT security performance. Rather, the key is effectively incorporating IT security in agency management actions and early in the life of IT systems.

Through the FY 2005 budget process agencies will identify the funding needed to correct specific security deficiencies that have been identified under the FISMA reporting process and included in agency POA&Ms.

Enterprise Wide Initiatives Positively Impacting Security

Federal Enterprise Architecture

In addition to agency-centric efforts, OMB is championing enterprise wide initiatives to encourage adoption of secure technologies. The Federal Enterprise Architecture (FEA) currently being developed will enable system developers to better manage security and privacy considerations. The FEA framework consists of five reference models, performance, business, information, technical and data. Each of these models will have key intersections with security as well as privacy, including:

- Performance metrics to identify and monitor progress in closing IT security gaps
- Lines of business to identify mission-critical security requirements
- Information and data by line of business to identify sensitive information that requires security and privacy protection; and
- Components and technical requirements to ensure and enhance IT security.

OMB will continue to work with agencies through the FEA framework and individual agency architectures to ensure IT security and privacy considerations are identified, prioritized, and managed.

NIST Standards and Guidelines

In 2002-2003, NIST published 12 security guidelines covering a wide variety of topics such as email, firewalls, telecommuting and contingency planning. NIST also published 10 draft guidelines for review by Federal departments and agencies concerning topics such as certification and accreditation, awareness and training, and considerations in Federal Information technology procurements. In accordance with its responsibilities under FISMA, the National Institute of Standards and Technology published draft *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standard 199). This proposed standard will be used by all agencies to categorize systems according to risk level. NIST is also drafting companion guidelines recommending the types of information systems to be included in each category as well as minimum information security requirements.

Security Testing

NIST has utilized the Cryptographic Module Validation Program (CMVP) to test a number of new algorithms that use the Advanced Encryption Standard. The CMVP has now validated over 500 modules, with another 100 or more expected within the next year. This successful program utilizes private sector accredited laboratories to conduct security conformance testing of cryptographic modules against the cryptographic Federal standards NIST develops and maintains. To give a sense of the quality improvement that the program achieves, NIST statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without the NIST program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography.

In addition, in recent years, NIST, along with many others, have worked to develop the "Common Criteria", an international standard which can be used to specify security requirements. These requirements, developed by either users or vendors, are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the National Security Agency (NSA) in a program known as the National Information Assurance Partnership (NIAP). The *National Strategy to Secure Cyberspace* calls for a review of the NIAP to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. NIST has already begun staff discussions with NSA to identify ways that they might improve the process, and to understand the resources needed for NIAP to fully succeed.

SmartBUY initiative

This month, OMB announced its SmartBUY initiative which will allow the federal government to leverage its buying power to achieve maximum cost savings on commercial software packages. Because of its widespread use, anti-virus software was among the first group of packages selected for enterprise wide licensing. Antivirus software is currently purchased using license agreements with terms and prices that vary based on volume. For one popular brand of desktop antivirus software, an agency paid \$6.75 per seat, while a much larger department paid 35 cents (a 95 percent difference). It is OMB's belief that coordinated use of the best-priced software licenses will reap significant savings for the federal government.

E-Authentication Initiative

Through the E-Authentication e-government initiative, the Administration certified and accredited an e-Authentication capability early this year. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls

across government. OMB will also release draft e-authentication guidance for agencies which will ensure that electronic transactions have the appropriate type of authentication.

Federal Cyber Service: Scholarship for Service (SFS)

The National Science Foundation's Scholarship for Service program provides funding to colleges and universities so that they can award two year scholarships in the information assurance and computer security fields. Upon graduation, recipients must work for a federal agency for two years in fulfillment of their Federal Cyber Service commitment. Scholarship recipients are hired as information technology specialists and help to protect the U.S. Government's information infrastructure. This year, 39 graduates have been placed in federal agencies.

DHS' National Cyber Security Division

The Department of Homeland Security in implementing the President's *National Strategy to Secure Cyberspace* and the Homeland Security Act of 2002, has created the National Cyber Security Division under the Department's Information Analysis and Infrastructure Protection Directorate. The Division will provide for 7 x 24 functions, including conducting cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. The new division will provide additional information to OMB in support of its enforcement and compliance activities. This Division represents a significant step toward advancing the Federal government's interaction and partnership with industry and other organizations. The National Cyber Security Division builds upon the existing capabilities transferred to DHS from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System. The creation of this Division strengthens government-wide processes for incident response and improves protection of critical cyber assets through maximizing and leveraging the resources of these previously separate offices.

Patch Authentication and Dissemination Capability

At the present time, thirty-seven agencies subscribe to DHS' Patch Authentication and Dissemination Capability through the Federal Computer Incident Response Center (FedCIRC). This service validates and quickly distributes corrective patches for known vulnerabilities. As part of the new NCSD, FedCIRC will continue to build upon and expand this capability.

In a June 6th article, Federal Computer Week remarked that the Bugbear worm had not adversely impacted federal agencies. The Department of Defense noted that this was because they "continuously and rapidly take proactive measures." In general, agencies have improved their protection against malicious code by installing patches, blocking executables at the firewall, and using anti-virus software with automatic updates.

Conclusion

In closing, OMB is committed to a federal government with secure information systems. Due to the significant work of Federal agencies and IGs, we are able to point to real advancement in closing the Federal government's IT security performance gaps. That said, many pervasive IT security weaknesses remain, leaving the Federal government with significant risks. OMB will continue to work with agencies, Congress and the GAO to ensure that appropriate risk-based and cost-effective IT security programs, policies and procedures are put in place.