STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
HOUSE SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES AND THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, OF THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

February 14, 2008

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the status of the Federal government's efforts to safeguard our information and systems.

My remarks today will focus on the progress we have made in improving the security of the government's information and information technology (IT) systems as well as our strategy for managing the risk associated with our government services in this ever changing IT environment. In our increasingly interconnected and interdependent environment, security risks left unaddressed by one agency can exponentially compound security risks faced by all of us. Weaknesses in information security and privacy programs prevent agencies from achieving program goals and erode the public's trust in us and our services.

Information security and privacy are extremely important issues for the Administration. On March 1st, the Office of Management and Budget (OMB) will provide our fifth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). This report will go into detail on our improvements and remaining weaknesses for both security and privacy.

Each year, OMB provides to the agencies specific guidance for reporting on the status and progress of their security programs. We use this data to oversee their programs, evaluate security and privacy overall, and develop our annual FISMA report. As in the past, this year's guidance included both quantitative and qualitative performance measures related to the major provisions of FISMA and to agency privacy program requirements. In addition to the questions and measures included in previous years, this year OMB used the FISMA reporting vehicle to gather Inspectors General's (IG's) assessments of the quality of agency Privacy Impact Assessments (PIAs) processes.

Over the past year, departments and agencies continued to improve their security programs, manage their risk and become more fully compliant with FISMA. An increasing number of agency systems completed certification and accreditation and annual testing of their security controls. In addition, agency IGs reported improvements in the quality of certification and accreditation and agencies' corrective plans of action and milestones. Agencies continued to improve their privacy programs.

In addition to information security progress, the Federal government has been making progress in implementing the April 2007 recommendations of the President's Identity Theft Task Force. Specifically, we have required agencies to review the use of Social Security Numbers (SSNs), underscored data security guidance – including encryption of portable storage and encryption devices.

On May 22, 2007, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." M-07-16 required agencies to complete their review for the use of SSNs and to identify instances in which collection or use of the SSN is unnecessary. Within 120 days from the date of the memo, M-07-16 required agencies to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. OMB is working with SSA and other agencies to explore alternatives to agency use of SSNs as a personal identifier in Federal programs. For Federal employees, OPM is leading the effort to develop policy for employee identifiers to minimize risk of identify theft.

In addition to M-07-16's requirement to complete the survey for the use of SSNs, the memo included reminders to encrypt all data on mobile computers/devices carrying agency data, unless the data is determined, in writing by the Deputy Secretary of each department, to not to be sensitive. This reminder would include agency laptops and other devices which contain personal information. Per this requirement, the encryption must be the National Institute of Science and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 certified. To implement FIPS 140-2, or Security Requirements for Cryptographic Modules, NIST has developed a testing and certification program to ensure the encryption algorithm being used in the product is secure. All encryption must pass this certification process.

How Do We Oversee Agency Performance?

In addition to the annual FISMA reporting process, OMB continues to use the oversight mechanisms described below to improve agency and government-wide IT security performance.

President's Management Agenda Scorecard

The President's Management Agenda (PMA) Expanding Electronic Government (E-Government) Scorecard includes quarterly reporting on agencies' efforts to meet their security goals. Agencies must provide OMB with a quarterly update on IT security performance measures and Plan of Actions and Milestones (POA&M) progress. The quarterly updates enable the agency and OMB to monitor agency remediation efforts and identify progress and problems.

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html.

Scorecards are also used to track agency progress in improving privacy programs and practices. In each Agency's Third Quarter of FY 2007 E-government scorecard, OMB included language that required Chief Information Officers (CIOs) to certify compliance with M-07-16. Due to agency difficulties in certifying compliance so shortly after the issuance of M-07-16, OMB required agencies in the Fourth Quarter scorecards to submit a status update by December 14th as well as a date when the agency would be in full compliance of the M-07-16 requirements, such as development of a breach notification policy and incident reporting requirements. The Fourth Quarter scorecards also required CIOs to certify that they had reminded agency staff to protect laptops and other portable data storage and communication devices.

Review of Agency Information Technology Investment Requests

Several years ago, OMB integrated information technology security into the capital planning and investment control process to ensure security was built into and funded over the lifecycle of each agency system. This also helps promote greater management attention to security as a fundamental priority. To guide agency resource decisions and assist oversight, OMB's policies require agencies to:

- Report security costs for all information technology investments;
- Document adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Additionally, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and the NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

This year, when reviewing investments, we considered the IG's annual review of the quality of the agency's C&A process. If the process was not considered "satisfactory" or better by the agency IG, the agency's investment portfolio was placed on our Management Watch List to continue the necessary management oversight.

Ongoing Security and Privacy Initiatives

As agencies continue to improve their security and privacy metrics reported quarterly and annually, we are striving to help agencies with their operational security and privacy processes by providing cross-agency tools and collaboration opportunities. Recently, we've engaged agencies in several new initiatives building upon the foundation of the activities associated with FISMA and privacy compliance processes. New and existing initiatives to help agencies improve their security and privacy posture have been well received, and are entering the implementation phase across agencies. These initiatives, which I will discuss in greater depth throughout this testimony, aim to improve security and privacy while allowing agencies to implement requirements in a more cost effective manner.

Federal Desktop Core Configuration (FDCC)

Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops which are running Microsoft Windows XP or VISTA. This set of controls, known as the Federal Desktop Core Configuration (FDCC) is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems, and allowing for closer monitoring and correction of potential vulnerabilities. Security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. In particular, security configurations help protect connections to the Internet and limit the download of Internet applications to only authorized professionals.

In addition to the desktop configuration, we are also working with the vendor community to make their applications safer. As part of this program, NIST has developed testing tools for use by both Federal agencies and vendors. NIST awarded Security Content Automation Protocol (SCAP) Validation to three products as of February 4th, 2008. These products and their associated validation information can be found at http://nvd.nist.gov/scapproducts.cfm. Three independent laboratories have been accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) for SCAP Product Validation testing. The list of accredited labs is available at the same URL. We are very optimistic this program will greatly enhance the security of our Federal desktops, and, of our Federal enterprise as a whole. We are requiring agencies use these tested products, and to help agency procurement officers with this requirement, we have provided agencies with recommended procurement language. This language can be found in our Memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf. Currently, the Federal Acquisition Council is in the process of adding similar language to the Federal Acquisition Regulation.

Trusted Internet Connections

Agencies connect to the Internet to deliver timely information and services to the public, however, our Government systems are continuously operating under increasing levels of risk. Each new external connection increases threats and vulnerabilities faced by agencies, and reports are demonstrating we are experiencing consequences such as loss of public confidence. Through the Trusted Internet Connections (TIC) initiative, we are working with agencies to reduce the overall number of external Federal connections, in order to manage our risk and secure our connections in a more cost-effective and efficient manner to provide better awareness of our environment. Agencies turned in plans of action and milestones to fully optimize agency connections, with a target completion date of June 2008.

As agencies optimize their external connections, security controls to monitor threats must be deployed and correlated to create a government-wide perspective of shared risks to our networks. The Department of Homeland Security (DHS) supports an application named Einstein to collect, analyze, and share aggregated computer security information across the Federal government. Einstein will assist agencies to raise their awareness and DHS for government-wide awareness for information security threats and vulnerabilities. This awareness will enable agencies and DHS to take corrective action in a timely manner. We are currently working with DHS to build upon their existing deployments and extend Einstein to all of the Federal agencies.

Information System Security Line of Business (ISSLOB)

Through the ISSLOB, introduced in the Spring of 2005, an inter-agency task force identified common solutions to be shared across government and developed a joint business case outlining a general concept of operations with overall milestones and budget estimates. The Task Force identified common solutions in four areas: security training; FISMA reporting; situational awareness/incident response; and selection, evaluation and implementation of security solutions. All agencies were asked to submit proposals to either become a Shared Service Center (SSC) for other agencies, or migrate to another agency from which they would acquire expert security services. DHS helped coordinate the selection of SSCs, and agency implementation of these services.

As of November 2007, 12 agencies had implemented security awareness training services provided by the initiative, and 13 agencies had begun using FISMA reporting services provided by the initiative. As a result, agencies are beginning to reduce duplicative investment in common security tools, ensuring a baseline level of training and reporting performance, and are able to refocus their efforts to other complex and critical security issues at their agency. OMB expects agencies will fully report the number of employees trained via the ISSLOB in their fiscal year 2008 annual FISMA report.

With the work completed to date in the ISSLOB, the TIC initiative, implementation of IPv6 and Homeland Security Presidential Directive (HSPD) 12, and the Federal government's initiative to implement the secure desktop configurations (i.e., FDCC), the Federal government is raising the bar of our security posture for our information and IT systems. OMB intends to continue using the ISSLOB to achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable.

SmartBUY and Blanket Purchase Agreements

SmartBUY is a Federal government procurement vehicle designed to promote effective enterprise level software management. By leveraging the government's immense buying power, SmartBUY can potentially save taxpayers millions of dollars through government wide aggregate buying of Commercial Off the Shelf (COTS) software products. Agencies are utilizing new SmartBUY agreements to àcquire quality security products at lower costs. In one recent example, GSA and DOD established a SmartBUY agreement for NIST certified products which will encrypt data at rest. This not only benefits Federal agencies, since the Blanket Purchase Agreement (BPA) was written so that states and local governments can also take advantage of this opportunity.

In addition to the encryption BPA, GSA worked to complete two BPA's for credit monitoring services deemed necessary by an agency in the event of a breach of personally identifiable information (PII), as well as risk assessment services for when a breach occurs. More information about the BPA related to credit monitoring services can be found in our OMB Memorandum M-07-04, "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf. More information about the BPA aimed at helping agencies to better respond to PII incidents and breach notifications can be found in our OMB Memorandum M-08-10, "Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2008/m08-10.pdf. Currently, the ISSLOB is working across Federal agencies and with GSA, to assess the feasibility of additional security related SmartBUY and BPA opportunities for situational awareness and discovery tool sets.

H.R. 4791

Recently, we provided the opportunity for all departments and agencies to review proposed legislation, H.R. 4791, entitled, "Federal Agency Data Protection Act." The bill contains several provisions that aim to enhance the protection of Federal information and personally identifiable information, as well as several provisions that propose changes to the FISMA. While we strongly support enhancing protections for such information we share several concerns expressed across Federal agencies about the effect of this legislation. The Administration believes the foundation and framework established by FISMA is sound, and also believes that there is still much we can accomplish to improve the security and manage the risk associated with our information and information services. Nonetheless, we are concerned that the unintended consequences of the proposed changes would seriously impact established agency security and privacy practices while not necessarily achieving the outcomes of improved privacy or security. Additionally, while we recognize that technologies that are improperly implemented introduce increased risk, we recommend any potential changes to the statute be technology-neutral. We recognize that the IT landscape is ever changing. As we deploy common, government-wide solutions, departments and agencies increasingly are acquiring services instead of procuring infrastructure. We welcome the opportunity to further discuss potential gaps that may need to be addressed through future FISMA enhancements, if appropriate. We look forward to discussing our ongoing information security and privacy activities in greater detail. We feel our current activities and initiatives – as described above – already are beginning to close performance gaps H.R. 4791 attempts to address.

Conclusion

Over the past year, agencies made steady progress in closing the Federal government's information and IT systems security performance gaps. Analysis of baseline performance measures indicates policy compliance improvements in a number of programs.

As part of its oversight role, OMB will continue to use quarterly reporting mechanisms along with agency information technology budget planning documents to track key performance metrics for FISMA and privacy compliance. Agency status and progress will be reflected on the President's Management Agenda scorecard.

Finally, the Administration intends to continue our efforts to build upon and provide cross-agency tools and collaboration opportunities through our ongoing information security initiatives. By implementing solid information security solutions across the government, we can address risks and improve security in a cost effective manner. We look forward to your continued support in these areas, and appreciate the attention you've brought to Federal information security and privacy issues.