EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

June 7, 2007

Good morning, Chairman Towns, Chairman Clay and Members of the Committee. Thank you for inviting me to discuss the status of the Federal government's efforts to safeguard our information and information systems.

Good security and privacy are shared responsibilities. As you know, within a framework of laws developed by Congress and through direction from the President, the Office of Management and Budget (OMB) develops policies for and oversees agencies' programs to protect information security and privacy. Agencies are responsible for implementing the policies based upon the risk and magnitude of harm that would result from a breach in their security, ensuring their programs are managed to maintain risk at an acceptable level, and Inspectors General must independently evaluate effectiveness of agency programs and processes. In addition to agency responsibility, each agency employee - from rank and file employees and their supervisors to independent evaluators and overseers must be held accountable for performing their assigned responsibilities, which include the protection of information security and privacy. Security and privacy are commonly seen as separate responsibilities and programs. They are not. We see them as separate pieces of the same puzzle – personally identifiable information is an example of what to protect, while security is a program for how to protect it.

In March 1, 2007, OMB issued our fourth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). My remarks today will focus on the progress we have made in improving the security and privacy for government information through Agencies' security and privacy programs, as well as our strategy for addressing continuing challenges. While the FISMA report characterizes our overall programmatic progress, OMB has taken a number of additional steps to improve the security and privacy of government information through effective use of policy tools and our Government-wide management processes. I will outline some of these initiatives later in my testimony.

Overall, Departments and agencies continue to improve their programs. An increasing number of agency systems have a completed certification and accreditation, a defined risk impact level, and a tested set of security controls and contingency plans. In addition, the majority of agencies report having appropriate oversight in place for their privacy programs. However, our view of the state of government security is much the same as reflected in your Committee's annual security report card: programs require additional improvements in implementation.

Progress in Improving Agency Security Programs

This year, as in past years, OMB provided agencies specific guidance for reporting on the status and progress of their security and privacy programs. The reports provide us quantitative and qualitative performance measures to continually assess agency security and privacy programs, and are used to develop our annual FISMA report.

The FY 2006 agency FISMA reports identify progress by individual Departments and agencies in the following areas:

- Certification and accreditation of systems. This past year, the number of systems with formal management approval to operate rose from 85 percent to 88 percent. The Department of Homeland Security and Department of State have made outstanding progress in certifying and accrediting their systems. Thirteen agencies now report a certification and accreditation rate of 100% of operational systems. Based on agency reports, a higher percentage of high impact systems have been certified and accredited. This potentially demonstrates agencies are working first to secure the systems presenting the highest risk.

- Testing of security controls and contingency plans. The number of systems with completed annual testing of system controls increased by 25 percent. Agencies tested security controls for 88 percent of systems and contingency plans for 77 percent of all systems, up from 61 percent and 72 percent respectively in FY 2005. The Department of Defense (DOD) alone increased system testing by more than 30 percent.

- Security Awareness Training. Agencies reported increases in the percentage of employees receiving security awareness training and for employees with significant information security responsibilities, up 10 percent and 3 percent respectively from the prior year.

The FY 2006 agency FISMA reports reveal modest success in meeting several key privacy performance measures:

- Program Oversight. In 2006, the majority of agencies report having appropriate oversight over their privacy programs in place. All agencies report having a privacy official who participates in privacy compliance activities, although 84 percent report coordinated oversight with their IG. Most agencies report privacy

training for Federal employees and contractors, with 92 percent reporting general privacy training and 84 percent reporting job-specific privacy training.

- Privacy Impact Assessments. The Federal goal is for 90 percent of applicable systems to have publicly posted privacy impact assessments (PIA). In 2006, 84 percent of applicable systems government-wide has publicly posted privacy impact assessments. 88 percent had written processes or policies for all listed aspects of PIAs.

- System of Records Notices. The Federal goal is for 90 percent of applicable systems with personally identifiable information contained in a system of records covered by the Privacy Act to have developed, published, and maintained systems of records notices (SORN). In 2006, 83 percent of systems government-wide with personally identifiable information contained in a system of records covered by the Privacy Act have developed, published, and maintained current SORNs.

Securing Agency Personal Identifiable Information (PII)

In 2006, several agencies experienced high profile data security breaches involving PII. OMB's Deputy Director for Management, Clay Johnson, testified last June before the Committee on Oversight and Government Reform and described the inter-relationship between security and privacy programs. Personally identifiable information is an example of what to protect, while security is a program for how to protect it.

As part of the agency information security program, cyber security incidents are reported to the Department of Homeland Security's (DHS') US-CERT response center. The agency agreed upon definition for reportable cyber incident includes loss or breach of PII. DHS reports 40 Departments and Agencies have reported to them over 3.900 separate security incidents involving PII to date this fiscal year (through June 5, 2007). Virtually all of these incidents resulted from "internal" problems within agencies and not external attacks on agency systems.

To help address the above issues, in May 2006 the President signed Executive Order 13402, entitled "Strengthening Federal Efforts to Protect Against Identity Theft," which created the Federal Identity Theft Task Force chaired by the Department of Justice and co-chaired by the Federal Trade Commission. On April 23, 2007, the taskforce submitted a strategic plan to the President outlining steps the Federal government can take to combat identity theft. This plan, titled "Combating Identity Theft: A Strategic Plan" is available at www.idtheft.gov. In this document, the Task Force recommended better education for Federal agencies on how to protect their data and monitor compliance with existing guidance. In this regard, OMB and DHS, through the Information Systems Security Line of Business (ISS LOB), is developing a document to outline best practices and develop a list of the most common mistakes to avoid in protecting information held by the government.

OMB issued four security and privacy policy and advisory memoranda in fiscal year 2006 which:

- directed the Senior Agency Officials for Privacy for Federal agencies to conduct a review of policy and processes, train agency employees, and report to OMB in October with their annual FISMA reports;
- asked agencies to implement certain security controls within 45 days to protect remote information, including encryption for mobile devices, two factor authentication, time out functions, and data extracts;
- required agencies to report the loss of personally identifiable information within one hour and reminded agencies of longstanding policy which requires security controls to be funded within each system; and
- provided suggested steps for planning and responding to data breaches which could result in identity theft.

In October 2006, the Inspector General (IG) community assessed agencies' status in meeting the recommendations for remote access of sensitive agency information. Agencies have made progress in verifying or ensuring the adequacy of organization policy, but much work remains. We are currently in the process of working with the IGs to obtain an updated assessment of status and in this area. The implementation challenges are not insignificant and the agencies show mixed results on OMB's request for additional actions.

On May 23, 2007, OMB issued policy M 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which directs Federal agencies to develop and implement a risk-based breach notification policy within 120 days, while ensuring proper safeguards are in place to protect the information.

Additionally, this memorandum directs agencies to:

- review and reduce current holdings of all personally identifiable information;
- review the use of Social Security Numbers to identify instances in which collection or use of the SSN is superfluous;
- establish a plan to eliminate the unnecessary collection and use of SSNs (this plan must be implemented within 18 months);
- participate in Government-wide efforts to explore alternate personal identifiers,
- protect Federal information accessed remotely;
- develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and potential corrective actions for violations; and
- train employees regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities.

This memorandum recognizes that safeguarding against breaches from happening in the first place has greater value than responding to breaches when they occur.

Accordingly, the Federal government should not unnecessarily collect or maintain personally identifiable information.

Continuing Challenges in Implementing FISMA

While progress has been made by most agencies, reports continue to identify a number of deficiencies in agency security procedures and practices. Deficiencies are most frequently seen in overseeing contractors, and the quality of certification and accreditation and POA&M processes.

- Maintenance of accurate system inventories and contractor oversight. IGs reported a slight decrease in the number of agencies with a system inventory over 80 percent complete, from 21 in 2005 to 20 in 2006. Though the majority of agency IGs reported inventories to be 96-100 percent complete, some agencies are still demonstrating large fluctuations in the number of systems in their inventories, both upwards and downwards. This makes it unclear whether all agencies have a handle on the universe of their information and information systems. OMB asked IGs to confirm whether the agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and National Institutes of Science and Technology (NIST) guidelines. Through IGs' evaluation of the inventory, we will have a better sense of whether or not Agencies are securing all of their information and information technology.

- Quality of certification and accreditation and Plan of Action and Milestones (POA&M) processes. Certification and accreditation and POA&M processes are important aspects of an agency information security program to assess risks, implement controls, and track corrective actions and risk mitigation. While these processes do not "guarantee" security, they help to ensure that weaknesses in information systems and programs are identified and managed well. IGs reported an overall decrease in the quality of the certification and accreditation process from 2005, where 17 agencies were reported as "satisfactory" or better, yet the number of agencies moving to the "good" and "excellent" categories increased in 2006. OMB policy requires agencies to prepare documentation (POA&Ms) for all programs and systems where a security weakness has been found, and asks agency IGs to evaluate this process. Based on OMB analysis of IG reports, no overall progress was made except that agencies that are rated as having effective processes are more often rated as being "almost always" effective rather than "mostly" effective. OMB encourages CIOs and IGs to work together to remediate these process weaknesses, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Assignment of a risk impact level. Agencies reported a total of 10,595 systems categorized by a risk impact level of high, moderate, low, or undetermined. The number of systems categorized increased this year from 91 percent to 93 percent.

Yet, as of October 2006, 331 agency systems and 369 contractor systems had not yet been assigned a risk impact level. OMB recognizes that in order for a system to be adequately protected, the potential level of impact that system could have to an agency must be determined. OMB will continue to measure this requirement.

In addition to deficiencies noted by the agency IGs, we have identified areas of concern through our own reviews and in consultation with other experts including the agencies and the Government Accountability Office (GAO):

- Government-wide implementation of general and job-specific privacy training for Federal employees and contractors;
- Maintenance of current PIAs and SORNs for 90 percent of applicable systems;
- Implementation of privacy policies and practices, and
- Improved oversight coordination between agencies and IGs.

Activities to Improve IT Security Performance

IT Security Line of Business

The Information Systems Security Line of Business (ISS LOB) assists agencies in identifying and consolidating common security processes and technologies to improve the Government's security and privacy performance, while also increasing efficiency and reducing cost.

Last year, the initiative facilitated a competitive and analytic process to select the Department of Defense (DoD), the Office of Personnel Management, and the Department of State (in coordination with the United States Agency for International Development) as security awareness service providers. Additionally, two agencies were selected as shared service providers to support FISMA reporting processes; the Department of Justice and the Environmental Protection Agency.

Service providers demonstrated an ability to provide information security products and services on a Government-wide and cost-effective basis. Agencies are now selecting their service providers and using them.

Standard Identifications for Federal Employees and Contractors

I would like to mention longer-term steps we are taking to increase the security of our sensitive information, computer systems, facilities, and employees. In response to an August 2004 Presidential directive, OMB led the development of a common identification standard for several million Federal employees and contractors. This directive requires all Executive branch agencies to conduct background checks on their employees and contractors before issuing them permanent government identification. The agencies are in the process of conducting these checks, and they began issuing new identification cards in October, 2006. These cards have built-in security features to

control access to Government computer systems and the Government's physical facilities.

President's Management Agenda Scorecard

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

The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of performance in all the criteria), or red (agencies have any one of a number of serious flaws).

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

To "get to green" under the Expanded E-Government Scorecard, agencies must meet the following three security criteria:

- IG or Agency Head verifies the effectiveness of the Department-wide IT security remediation process;
- IG or Agency Head rates the agency certification and accreditation process as "Satisfactory" or better; and
- The agency has 90 percent of all IT systems properly secured (certified and accredited).

In order to "maintain green," by July 1, 2007, agencies must meet the following security and privacy criteria:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations; and
- Has demonstrated for 90 percent of applicable systems a PIA has been conducted and is publicly posted; and

- Has demonstrated for 90 percent of systems with personally identifiable information contained in a system of records covered by the Privacy Act to have developed, published, and a maintained current SORN.

OMB will continue to use the E-Government scorecard to assess agency progress and highlight areas for improvement.

Review of Agency Information Technology Investment Requests

FISMA requires agencies to ensure information security is addressed throughout the life cycle of each information system, and several years ago OMB included this policy into Circular A-11, our primary budget guidance to the Agencies, to incorporate of the costs for security in the lifecycle of information technology capital investments.

When determining whether funding of agency investments is justified, we review whether agency capital planning documentation adequately demonstrates how each investment addresses the requirements of the FISMA, Privacy Act, OMB policy, and NIST guidelines, as appropriate. This procedure also helps agencies ensure information security management processes are integrated with agency strategic and operational planning processes.

For example, agencies must demonstrate:

- security costs are incorporated in to the life-cycle costs for each investment;
- security controls (e.g., certification and accreditation, security testing, and contingency plans) are completed and up to date;
- contractor security procedures are monitored and validated;
- security weaknesses are incorporated into the agency's plan of actions and milestones process;
- system of records notices are completed and up to date; and
- privacy impact assessments are completed, up to date, and published for the public to review.

GSA SmartBuy Initiative

Through the GSA SmartBuy initiative, we are working to help agencies procure better information security and privacy tools at a lower cost. Recently, we completed a SmartBuy for anti-virus software, and, are nearing completion on a SmartBuy for FIPS 140-2 certified encryption tools.

Adoption of Common Security Configurations

OMB recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," requiring agencies to adopt standard security configurations for Windows XP and VISTA

by February 1, 2008. These configurations were established collaboratively by Microsoft, NIST, DHS, and DoD.

Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information.

A number of concurrent activities will further assist agency adoption of common security configurations. NIST and DHS continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers access to Windows XP and VISTA images. The images will be pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.

Additionally, OMB provided recommended language for agencies to use to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations.

Conclusion

I have outlined above a number of actions we are taking to demonstrate the Administration takes its information security and privacy responsibilities very seriously. These will help prevent security incidents, permit us to better respond if prevention fails, and provide us a more complete and timely view of agency performance. Agencies spend more than $6.0 billion each year on controls to protect information and computer systems. We will use the budget process to ensure this money is wisely spent and re-emphasize new spending on information technology will not be approved if sound security is not already in place for existing systems and programs. OMB encourages CIOs, Senior Agency Officials for Privacy, and IGs to work together to remediate deficiencies.

Finally, the Administration intends to focus on protecting the personal information of our citizens. Information security, when implemented correctly, results in the protection of all information, including personal information.

I look forward to working with you to improve our security and privacy programs and welcome any suggestions you have.