STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION, FEDERAL SERVICES, AND
INTERNATIONAL SECURITY

March 12, 2008

Good afternoon, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the state of Federal information security, and the implementation of controls to improve information security.

Securing Federal information and information systems has been an Administration priority, and over the last several years we have focused management attention on improving our security processes and protection measures. We have approached the challenges presented in our Federal operating environment by building a strong Federal information security framework. This framework stresses implementation of risk-based and cost-effective information security controls to provide the appropriate levels of information protection. Since the passage of the Federal Information Security Management Act of 2002 (FISMA), we continue to make progress. Throughout this testimony, we will highlight our results, and briefly describe some of our initiatives intended to close remaining performance gaps.

Information Security Progress and Priorities

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). This law, and the resulting policies and guidance, set a base framework from which agencies have developed their information security programs. OMB policies and subsequent National Institute of Standards and Technology (NIST) guidance focus on a risk-based, cost-effective approach and reflect the balance between strong security and mission needs. As required by 44 U.S.C. § 3543, Federal agencies must comply with standards developed by NIST and promulgated by the Secretary of Commerce, and identify information security protections consistent with these standards. Agencies are responsible for implementing the policies and guidance for their unique mission requirements within their capital planning and investment control processes. Agency officials who manage and operate the agency business programs are ultimately responsible and accountable for ensuring security is integrated into those program

operations. Our oversight is achieved in two primary ways -- via the budget and capital planning process, and through independent program reviews.

On March 1, 2008, we submitted the Government-wide fifth annual report to Congress, entitled "Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002," http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf

Since 2002, we have been monitoring government-wide progress in implementing key FISMA performance metrics. We would like to note, in fiscal year 2007 we met a significant milestone by certifying and accrediting (C&A) over 90% of all systems. The C&A process, as described in NIST guidance, includes a comprehensive assessment of the management, operational, and technical security controls; and, an official management decision given by a senior agency official to authorize operation of an information system. The certification process is in place to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements and managing the system's risk to an acceptable level.

Baseline security controls for selection and testing throughout the system C&A have been outlined in NIST's Federal information security control catalog. Security control requirements are determined when agencies categorize their information and information systems for risk impact levels (high, moderate, or low). Systems containing information with higher risk impact level, have stronger required baseline controls than information systems containing less sensitive information.

As you can see in the table below, since 2002, we have increased our percentage of C&A'ed systems from 47% to 92%, while increasing the total number of systems by nearly 30%. Concurrently, we have also improved our rate of contingency plan testing and annual follow-up testing of system security controls. At the end of 2007, 80% of the 25 major agencies reported a C&A rate between 90% and 100% for operational systems. This makes it clear that progress is spread across Federal agencies and not limited to agencies with a large inventory.

Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2007

Percentage of Systems with a:	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**	**FY2007**
Certification and Accreditation	47%	62%	77%	85%	88%	**92%**
Tested Contingency Plan	35%	48%	57%	61%	77%	**86%**
Tested Security Controls	60%	64%	76%	72%	88%	**95%**
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	**10,304**

To validate the quality of agencies' self-reported metrics, we ask agency Inspectors General (IG) to assess the quality of the processes behind the reported

numbers. In fiscal year 2007, 76% of reporting agency IGs rated the overall quality of C&A processes to be "satisfactory" or better in fiscal year 2007, while the number of agencies with the lowest rating (poor) was reduced from 9 in fiscal year 2006, to 4 in fiscal year 2007.

In addition to gauging C&A completion and security control implementation at the system level, we are also working to strengthen security controls on Federal desktops. 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, 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.

To continue our trend of performance improvement, over the next year we intend to focus information security and privacy management attention on:

- Achieving 100% C&A levels for all operational systems;
- Properly identifying and providing oversight of contractor systems;
- Reducing or eliminating systems in the FISMA inventory uncategorized by risk impact level;
- Improving agency identification and reporting of security incidents;
- Increasing general and job-specific training for Federal employees and contractors;
- Maintaining appropriate privacy documentation for 90% of applicable systems; and,
- Completing activities related to privacy recommendations.

Securing Sensitive Information and Personally Identifiable Information

On June 23, 2006, we released Memorandum M-06-16, entitled "Protection of Sensitive Agency Information." (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf) In this memorandum, recommendations were made to compensate for the lack of physical security controls when sensitive information is removed from, or accessed from outside the agency location. The memo contained a requirements checklist, along with the following recommended actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

To make the Federal government's identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the President's Identity Theft Task Force issued "Combating Identity Theft: A Strategic Plan." The strategic plan instructed the OMB and the Department of Homeland Security (DHS) to develop a paper identifying common risks (or "mistakes") and best practices to help improve agency security and privacy programs. The risks, best practices, and important resources are inter-related and complementary. Agencies apply them when administering their information security and privacy programs. The report can be found at: http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf).

Subsequently, building on the work of the President's Identity Theft Task Force, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007. The purpose of Memorandum M-07-16 is to enhance agency protections on personally identifiable information through the establishment of agency breach notification policies and risk mitigation frameworks. Memorandum M-07-16 reiterated the recommended security measures from Memorandum M-06-16, and further required these actions to be taken as they relate to personally identifiable information.

In each agency's Fourth Quarter FY 2007 President's Management Agenda E-Government scorecard, OMB included language requiring agencies to submit a status update by December 14, 2007, as well as a date when each agency would be in full compliance of the M-07-16 requirements. We are working with agencies to refine these plans, and will continue to leverage the quarterly scorecard process as a management tool, to ensure agencies continue to improve required security control implementation.

Detecting Access to Federal Information Systems

While strong security controls can help reduce the number of information security incidents, experience shows some incidents and attacks cannot be prevented. Consequently, an effective incident detection and response capability is critical.

As shown in the table below, in fiscal year 2007, 12,986 incidents were reported to the DHS incident response center for six categories of incidents, which is more than twice the amount of incidents reported in fiscal year 2006.

Incident Reporting to DHS US-CERT			
Incident Categories	**FY 2005**	**FY 2006**	**FY 2007**
1. Unauthorized Access	304	706	2,321
2. Denial of Service	31	37	36
3. Malicious Code	1,806	1,465	1,607
4. Improper Usage	370	638	3,305
5. Scans/Probes/Attempted Access	976	1,388	1,661
6. Under Investigation	82	912	4,056
Total Incidents Reported	3,569	5,146	12,986

While the increasing number of reported incidents seems alarming, we are finding this increase to be at least partially attributable to improved incident identification and reporting. As agencies become more aware of their operating environment, they are likely to detect previously undetectable incidents.

To further improve situational awareness and incident detection, agencies are engaged in the Trusted Internet Connections initiative (TIC), and Einstein tool deployment. Through the Trusted Internet Connections (TIC) initiative, we are working with agencies to reduce the overall number of external connections, including Internet points of presence. As agencies optimize their external connections, security controls to monitor threats will be deployed and correlated to create a government-wide perspective of our networks. To facilitate monitoring of external connections, The Department of Homeland Security (DHS) supports an application named Einstein. Einstein is an intrusion detection system, able to collect, analyze, and share aggregated computer security information across the Federal government. Einstein will enhance current incident detection abilities, and will raise government-wide awareness of 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.

Conclusion

In conclusion, there is evidence agencies are making progress in the area of information security and the protection of sensitive information. We are improving the quality of information security processes across the Federal government, while concurrently improving our reported performance metrics and compliance with FISMA. To further strengthen our information security and privacy posture, we are actively engaging agencies in government-wide initiatives. Through these government-wide initiatives, we are enabling Federal agencies to better focus their information security activities and resources.