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

March 16, 2006

Good morning, Mr. Chairman and Members of the Committee. 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 technology as well as our strategy for addressing continuing security challenges.

This is an extremely important issue for the Administration. It is equally important to me both professionally and personally because some of the government-wide security performance metrics we use to evaluate the agencies are also part of my personal performance plan.

On March 1st, OMB issued our third annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). Much of the information I am discussing today is provided in more detail in our report.

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 and develop our annual FISMA report. As in the past, this year's guidance included quantitative performance measures for the major provisions of FISMA and for the most part were identical to past years' measures. Consequently, areas of improvement, as well as areas requiring additional management attention are easily discernable.

In addition this year, OMB used the FISMA reporting vehicle to aggregate privacy reporting requirements. The privacy questionnaire -- Section D of the FISMA reporting template -- consolidates reporting under the Privacy Act, the E-Government Act, Section 522 of the Consolidated Appropriations Act and various OMB guidance and policy issuances. OMB's findings and conclusions based on the agencies' privacy reports are contained in OMB's E-Government Report to Congress. OMB will meet with selected agencies over the course of the spring and summer to assist them in enhancing their privacy programs.

Over the past year, Departments and agencies continued to improve their security programs and more fully comply with FISMA. An increasing number of agency systems have received certification and accreditation and annual testing of their security controls. In addition, agency Inspectors General reported improvements in the quality of certification and accreditation and agencies' corrective plans of action and milestones.

Progress in Improving Agency Security Programs

The FY 2005 agency FISMA reports identify progress by individual Departments and agencies in the following areas:

Certification and accreditation of systems

The process for certifying and accrediting information systems is important because it includes assessing risk, developing plans to manage the risk, implementing and testing security controls to ensure they work as intended, and requires an agency manager to verify they understand any residual risk prior to authorizing system operations.

This past year, the number of systems with a formal management approval to operate rose from 77 percent to 85 percent. This improvement is especially notable since the actual number of reported systems increased 19 percent over the last year from 8,623 to 10,289. Several agencies in particular have made outstanding progress: the Department of Defense moved from 58 percent to 82 percent of systems certified and accredited and the Department of Veterans Affairs improved from 14 percent to 100 percent. I am especially encouraged the certification and accreditation percentage for high impact systems is 88 percent -- higher than overall certification and accreditation. This demonstrates agencies are prioritizing their systems and working first to secure the systems presenting the highest risk impact level.

Quality of certification and accreditation processes.

To ensure certification and accreditation achieves the desired outcome, we ask agency Inspectors General (IG) to report on the overall quality of their agency's process. This year, 17 of 25 IGs rated their agency's process as "satisfactory" or better, up from 15 agencies last year.

Quality of agency corrective plans of action and milestone process (POA&M)

OMB also asks IGs to evaluate the effectiveness of agencies' POA&M process for tracking security weaknesses. This year, 19 of 25 IGs rated their agency's process as effective. This is an increase from 18 agencies last year.

Assignment of a risk impact level

FISMA required the National Institute of Standards and Technology (NIST) to develop a number of new standards and guidelines to assist the agencies in securing their

information systems. Among them was a standard for assigning to each agency system one of three security impact levels. The three levels (i.e., high, moderate, or low) reflect the potential impact on organizations or individuals in the event of a breach of security (i.e., a loss of confidentiality, integrity, or availability). Using the impact levels, agencies are better able to prioritize their security needs.

For the first time this year, we asked agencies to report on their implementation of this NIST standard. Agencies have assigned impact levels to 94 percent of the 9,184 systems they manage and 65 percent of the 1,105 systems managed by contractors. For agency managed systems, 18 percent were categorized as high impact, 27 percent as moderate, and 49 percent as low. For contractor managed systems, 27 percent of these were categorized as high impact, 23 percent as medium, and 15 percent as low.

Agency-wide security configuration policy

FISMA requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Standardized configurations reduce system vulnerabilities and simplify security management. All 25 large agencies have an agency-wide security configuration policy in place.

Continuing Challenges

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 testing security controls, overseeing contractors, and incident reporting.

Testing of security controls

FISMA requires agencies to periodically test and evaluate information security controls to ensure they are effectively implemented. Although agencies tested security controls on an increasing number of systems (7,425 in FY 2005 as opposed to 6,515 in FY 2004), the overall percentage of systems with tested security controls dropped from 76% to 72%. It should be noted, however, the percentage of high impact systems tested was appreciably higher at 83%.

Oversight of contractor systems

Agency IT security programs apply to all organizations possessing or using Federal information or operating, using or having access to Federal information systems. Therefore, OMB asked IGs to confirm whether the agency ensures oversight of information systems used or operated by a contractor or other organization on behalf of the agency to ensure they met FISMA requirements. Eighteen of 25 IGs said their agency at least frequently performed such oversight. Six IGs said their agency only sometimes or rarely did so. One IG did not report in this area.

Incident Reporting

It is essential for agencies to share information on common vulnerabilities and FISMA requires agencies to report their security incidents to a central incident handling organization. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) is the designated central incident handling organization and they continue to find sporadic reporting by some agencies and unusually low levels of reporting by others. Less than full reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event, e.g., the widespread propagation of an Internet worm or an organized attack by an adversary.

How Do We Oversee Agency Performance?

OMB will continue to use the oversight mechanisms described below to improve agency and government-wide IT security performance.

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 Expanding E-Government Scorecard, agencies must meet the following three security criteria:

- Inspector General verifies the effectiveness of the Department-wide IT security remediation process;
- Inspector General 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, 2006, agencies must have:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations; and
- Consolidated and/or optimized all agency infrastructure to include providing for continuity of operations.

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

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 that 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 NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

Information System Security Line of Business (ISSLOB)

Over this past year, an inter-agency task force identified common solutions to be shared across government and developed a draft joint business case outlining a general concept of operations with overall milestones and budget estimates. The Task Force identified common solutions in four areas – training, reporting, incident response, and evaluating and selecting security products and services. All agencies were asked to submit proposals to either become a service provider (Center of Excellence) for other agencies, or migrate to another agency from which they would acquire expert security services. The Department of Homeland Security is continuing to serve as the program manager for this effort and will work with those agencies proposing to become centers of excellence to bring greater clarity to their proposals. OMB intends to use the ISSLOB to achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable.

Conclusion

Over the past year, agencies made steady progress in closing the Federal government's information technology security performance gaps. Analysis of baseline performance measures indicates policy compliance improvements in a number of programs. However, inconsistent implementation of security measures across the Federal government leaves weaknesses to be corrected. OMB encourages CIOs and IGs to work together to remediate these deficiencies.

As part of its oversight role, OMB will use quarterly reporting mechanisms to track key performance metrics for FISMA compliance. Agency status and progress will be reflected on the President's Management Agenda scorecard.

Finally, the Administration intends to focus on the implementation of an information security line of business to reduce costs and increase security effectiveness across government. The establishment of Centers of Excellence for security training and FISMA reporting will be a first step towards ensuring greater use of standardized products and services.