STATEMENT OF
THE HONORABLE KAREN EVANS
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

March 16, 2004

Good afternoon, Mr. Chairman, Ranking Member Clay, 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 will focus on the findings in OMB's FY 2003 Federal Information Security Management Act (FISMA) report and our strategy to address both reoccurring and new information technology (IT) security challenges.

Earlier this month, OMB issued our third annual report to the Congress on agency compliance with IT security requirements in law and policy. FISMA, like its predecessor the Government Information Security Reform Act (GISRA), continues to be a valuable tool in improving the state of Federal IT security – both the security of systems and promoting the protection of information.

In addition to continuing key provisions from GISRA such as the critical role of Inspectors General (IGs) in conducting independent evaluations as well as an increased focus on accountability, FISMA also introduced new provisions. In particular, FISMA directs the National Institute of Standards and Technology (NIST) to develop IT security guidelines in a number of key areas such as the creation of minimum security standards for agency systems. NIST has been actively working with agencies in the development of those standards per their statutory role in providing technical guidelines to Federal agencies.

Background on FISMA Reporting

As you know, FISMA directs Federal agencies to conduct annual IT security reviews and IGs to perform annual independent evaluations of agency programs and systems and report their results to OMB and Congress. OMB's report is therefore based primarily on the FY 2003 IT security reports submitted by agencies and IGs. To ensure consistent reporting across the government, OMB issued FISMA guidance, M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting", which included specific reporting instructions along with quantitative performance measures to more effectively

determine agency status and progress. These instructions for agencies and IGs remained nearly identical to FY 2002 and were mapped directly to the requirements in FISMA. As a result, status against the FY 2001 baseline is easily identifiable.

Other key elements in OMB's FISMA guidance include:

- Continuation of IT security performance measures. Agencies and IGs were charged to report the results of their work against a key set of IT security performance measures. These measures have proved extremely valuable in identifying agency strengths and weaknesses, prioritizing resource decisions, and assisting OMB in our oversight activities.

- Continuation of IT security remediation efforts. OMB guidance continued the requirement Federal agencies to develop plans of action and milestones (POA&Ms) for every program and system where an IT security weakness has been found. POA&Ms must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, identified by the agency, IG, GAO, or OMB, are tracked and corrected. These plans must be developed, implemented, and managed by the agency official who owns the program or system where the weakness was found. An important step for agencies to ensure that have sufficient resources to resolve their weaknesses is tying their system-level POA&Ms directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11). This step is essential to link the justification for IT security funds to the budget process.

- IG assessment of agency POA&M process. To ensure successful remediation of IT security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor remediation efforts. The FISMA reporting instructions requested IGs to assess whether or not an agency has a process in place that meets criteria laid out in OMB guidance.

Additionally, the OMB guidance highlighted new provisions introduced by FISMA:

- Stronger emphasis on configuration management. FISMA requires each agency to develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.

- Codifies requirement for ensuring continuity of system operations. FISMA codifies a longstanding policy requirement that each agency's security program (and particularly each system security plan) include the provision for the continuity of operations for information systems that support the operations and assets of the agency. FISMA explicitly includes in this requirement, information and information systems "provided or managed by another agency, contractor, or other source."

- Development and maintenance of an inventory of major information systems. FISMA amends the Paperwork Reduction Act regarding the major information systems (including major national security systems) operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of "major information system" is found in OMB Circular A-130.

  The FISMA amendments requires that the identification of information systems in this inventory include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. OMB's guidance directed agencies to leverage their enterprise architecture work to create this inventory.

Key Findings from FISMA Report

The OMB FISMA report identifies progress and IT security weaknesses in FY 2003. Agency status against government-wide IT security goals as well as key IT security performance measures in FISMA guidance is provided below.

Progress Against Government-wide IT Security Milestones

OMB established three government-wide goals in the President's FY 2004 Budget and recently provided an update against these measures in the President's FY 2005 Budget.

- **Goal 1** – By the end of calendar year 2003, all Federal agencies will have created a central remediation process to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected. Each agency IG will verify whether or not the agency has a process in place that meets criteria laid out in OMB guidance.
  Status – While each Federal agency does have an IT security remediation process, the maturity of those processes vary greatly. Out of the twenty-four CFO Act agencies, twelve agencies have a remediation process verified by their IG as meeting the necessary criteria. OMB will continue to work with the remaining Federal agencies to achieve the full goal in 2004. OMB emphasizes the importance of an IG verified process by including it as one of three criteria necessary for agencies to "get to green" for IT security on the Expanding E-Government Scorecard of the President's Management Agenda.

- **Goal 2** – By the end of calendar year 2003, 80 percent of Federal IT systems shall be certified and accredited.
  Status – At the end of 2002, 48% of Federal IT systems had been certified and accredited. This percentage increased to 62% at the end of 2003.

- **Goal 3** – By the end of calendar year 2003, 80 percent of the Federal government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment. While agencies have made improvements in integrating security into new IT investments, significant problems remain, particularly in ensuring security of existing systems.
  Status – At the end of 2002, over 60% of Federal IT systems planned and budgeted for IT security requirements as part of the overall development or maintenance of systems. This percentage increased to 78% at the end of 2003.

Agency Progress Against Key IT Security Performance Measures

As discussed, agencies were directed to report their performance against a key set of IT security performance measures. These measures reveal both areas of progress as well as weaknesses. The table below provides the government-wide status from FY 2001 through FY 2003 against a subset of these measures. The data in this table is based on information reported in agencies' FY 2002 and FY 2003 FISMA reports and represents a starting point to get a clearer picture of agency efforts. However, it is important to note that some IG reports called into question the quality of some of this work. Additionally, as some agencies do not have a robust enterprise architecture they may not have an accurate inventory of all of their systems. When reviewing this information, it is also important to recognize that the total number of agency systems tends to change from FY 2001 to FY 2003. A goal of the FY 2004 OMB FISMA guidance is to standardize more of the annual reporting, including clearer definitions to eliminate interpretation differences.

Government-wide IT Security Performance from FY 2001 to FY 2003

Agency	Total No. and % of Systems			No. and % of systems authorized for processing following certification and accreditation			No. and % of systems with security control costs integrated into the life cycle of the system			No. and % of systems for which security controls have been tested and evaluated in the last year			No. and % of systems with a contingency plan			No. and % of systems for which contingency plans have been tested		
	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03	FY01	FY02	FY03
TOTAL	7360	7906	7998	1953	3772	4969	3001	4914	6182	2447	4743	5143	2216	4334	5450	1228	2768	3839
TOTAL				27%	48%	62%	41%	62%	77%	33%	60%	64%	30%	55%	68%	17%	35%	48%

Federal agencies, OMB, the Congress, and GAO are able to track and monitor agency efforts using those measures. While the Federal government is heading in the right direction additional efforts are still warranted. For example, there are notable increases in the percentage of systems with security plans and the percentage of systems certified and accredited. However, many Federal systems do not have appropriate contingency plans in place to ensure continuity of operations. Another continuing area of concern is the low government-wide percentage of systems with tested contingency plans.

Increased Accountability is Critical to Improving IT Security

Even with the strong focus of both GISRA and FISMA on the responsibilities of agency officials regarding IT security, there continues to be a lack of understanding and therefore accountability for IT security performance within the Federal government. The law is very clear on this issue. The agency head is ultimately responsible for the security of their information and systems and is charged with ensuring that agency senior officials and the agency CIO fulfills their specific IT security responsibilities. Specifically, agency senior officials are responsible for providing security for the information and systems that support their operations and assets. They must ensure that the risk to their information and systems is assessed, appropriate controls to protect against the risk are identified, implemented, and tested, and IT security requirements are budgeted. The agency CIO is responsible for the agency-wide information security program, developing and maintaining IT security policies and procedures, IT security training, and assisting agency senior officials with their responsibilities as well as ensuring the security of the information and systems under the CIO's control.

However, agency and IG reports continue to identify a number of troubling government-wide issues and trends, such as:

- Agency and IG reports continue to identify the same IT security weaknesses year after year, some of which are seen as repeating material weaknesses.
- Additionally, while the Federal government appears to be doing a much better job at planning for the security of new IT investments, too many legacy systems continue to operate with serious weaknesses.
- As a result, there continues to be a failure to adequately prioritize IT funding decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development.

While there are a number of options available to address these concerns they must ultimately be addressed through improved accountability. Even though 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. Ensuring the security of most agency information and systems is not the sole responsibility of the agency CIO. The majority of IT spending within agencies is not on IT infrastructure and networks, traditionally owned and operated by CIOs, but rather on mission IT investments. In fact, historically, over 65% of the Federal government's IT investments are normally mission-IT related. It is within these systems that many weaknesses recur.

IT security is a shared responsibility and holding just one official accountable potentially weakens an agency's ability to properly safeguard its entire collection of IT investments. Through the President's Management Agenda, OMB has increased accountability for agency security performance; however, greater consistency within agencies is necessary.

Plan of Action to Improve Performance

While IT security clearly has a technical component, it is at its core an essential management function. Most of the Federal government's IT security weaknesses can be resolved through better management and accountability. Specifically, OMB will pursue the steps outlined below as a plan of action to both assist agencies in their IT security efforts, promote implementation of law and policy, as well as track status and progress.

Prioritizing IT Funding to Remediate IT Security Weaknesses

Long-standing OMB policy requires agencies to incorporate IT security in the development of both new and existing IT investments and demonstrate that action in their IT budget materials. Agencies must: 1) report security costs for their IT investments; 2) document in their business cases that adequate security controls have been incorporated into the life cycle planning of each IT investment; 3) reflect the agency's security priorities as reported in their POA&Ms; and 4) tie their POA&Ms for an IT investment directly to the business case for that investment.

Failure to appropriately incorporate security in new and existing IT investment puts the investment at considerable risk for funding. Most of these weaknesses can be found in operational systems that either have never been certified and accredited or systems that have an out-of-date certification and accreditation.

Information from agency and IG IT security reports directly inform the budget process. Specifically:

- Information from agency and IG reports along with their remediation plans identified both agency-wide and system specific IT security weaknesses. Agency POA&Ms provide the corrective actions with estimated costs the agency has determined will resolve those weaknesses.

- Information from IT budget documents, the exhibit 53 and 300, also identify whether appropriate steps to secure both new and legacy IT investments have been undertaken.

This information was particularly useful in prioritizing FY 2004 funding decisions. For example, agencies with significant information and system security weaknesses were directed to remediate operational systems with weaknesses prior to spending FY 2004 IT development or modernization funds. If additional resources are needed to resolve those weaknesses, agencies are to use those FY 2004 IT funds originally sought for new development.

Finally, while funding for IT security has increased from $2.7 billion in FY 2002 to $4.2 billion in FY 2003, historically, a review of IT security spending and security results has demonstrated that spending is not a statistically significant factor in determining agency security performance. Rather, the key remains to effectively

incorporate IT security in agency management actions and implement IT security throughout the lifecycle of a system.

Oversight of Agency IT Security through the President's Management Agenda Scorecard

The President's Management Agenda Scorecard is an important mechanism for both acknowledging agency IT security progress and highlighting significant problems. OMB uses agency IT security materials to help inform the quarterly assessment of IT security under the E-Government scorecard.

To "get to green" under the Expanding E-Government Scorecard for IT security, agencies must meet the following three criteria: 1) demonstrate consistent progress in remediating IT security weaknesses; 2) attain certification and accreditations for 90% of their operational IT systems; and 3) have their IG assess and verify their POA&M process.

In addition to receiving an annual report on agency performance against key IT security performance measures, beginning in December 2003, agencies started reporting each quarter on their status against a subset of those measures. These updates are sent to OMB along with agencies quarterly updates on their POA&M efforts and are also used to inform the quarterly assessment of the President's Management Agenda Scorecard. The PMA enables OMB to hold agencies, their senior agency officials, and CIO accountable for IT security performance.

FY 2004 OMB FISMA Guidance and Upcoming NIST Guidelines

As we progress into the fourth year of these annual IT security requirements, our goal is to move even more toward performance measurement. The ability to clearly determine outcomes and results is essential. Therefore, it is important that FISMA reporting instructions mature to focus on key IT security areas and collect the most useful information to inform agencies, OMB, and the Congress on the status of agency efforts to secure their systems and protect their information. Additionally, NIST is actively working on the development of new guidelines required under FISMA which will play a significant role in guiding technical implementation of agency IT security efforts.

As part of the development of OMB's FY 2004 FISMA guidance, we are focusing on the following three areas: 1) evolving the IT security performance measures to move beyond status reporting to also identify the quality of the work done. For example, being able to determine both the number of systems certified and accredited as well as the quality of the certification and accreditation conducted; 2) the independent evaluations by the IGs continue to be a source of indispensable information and further targeting of IG efforts to assess the development, implementation, and performance of key IT security processes are invaluable; and 3) providing additional clarity to certain definitions to eliminate interpretation differences within agencies and between agencies and IGs.

Measuring the effectiveness of processes and procedures is key. OMB is a strong advocate for documented and repeatable processes for security. We and other experts find certification and accreditation an especially important process because it includes all of the important elements for securing systems. These include identifying risk, effectively planning to manage risk, testing security controls to ensure they are working as intended, understanding interconnections, and planning for inevitable system disruptions and other contingencies. Moreover, a uniform certification and accreditation process across the agencies permits a greater understanding of implemented security controls among interconnected partners.

At the same time, we are equally concerned that merely measuring whether certification and accreditation has been performed, does not tell us the quality of such or whether security is actually improved. If certification and accreditation is truly important, and we think it is, we must not permit it to devolve to the paper chase of past security planning efforts.

Moving to more qualitative performance measures has been our goal since we established a government-wide security baseline. Therefore for the FY 2004 FISMA report, we will ask agencies to report the extent to which any serious security incidents (e.g., root compromises or widespread viruses and worms) occurred on certified and accredited systems and if so to identify the causes. This empirical data will permit the agencies, OMB, and Congress to identify specific areas for improvement.

This data will also permit us to establish a new qualitative performance baseline against which we can measure the future effectiveness of recent and planned NIST guidance required by FISMA.

Conclusion

I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. It is this effort that gives OMB and the Congress much greater visibility into agency IT security status and progress.

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains to improve the security of the information and systems that support the Federal government's missions. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.