

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
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
April 8, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the status of the Federal government's IT security. Through the requirements of the Government Information Security Reform Act (GISRA) and now the recently enacted Federal Information Security Management Act (FISMA), Federal agencies, OMB, the Congress, and the General Accounting Office (GAO) are able for the first time to clearly understand the Federal government's IT security strengths and weaknesses. For the purposes of today's hearing, I will provide the Committee with an update on both the government-wide progress realized in fiscal year (FY) 2002, and areas of continuing concern as well as the next steps OMB is undertaking with agencies to continue IT security performance gains.

I also wanted to inform you of a noteworthy E-government milestone. The March 17th Nielsen//NetRatings report which found that more than one-third of all Internet users visited a Federal government site in February. This finding is a clear indicator of the Federal government's commitment to maximizing the Internet to communicate with and provide services to Americans. The challenge that the Committee highlights at today's hearing is ensuring that the information and services are also appropriately secure.

As you know, GISRA has been instrumental in guiding Federal agencies toward greater IT security performance. Through GISRA and accompanying OMB guidance we have established a clear process to ensure effective management of IT security, sound implementation and evaluation of programs, procedures, and controls, along with appropriate and timely remediation of IT security weaknesses. OMB oversees and enforces these requirements through

traditional management and budget processes discussed later in my testimony.

Government Information Security Reform

GISRA brought together existing IT security requirements in previous legislation, namely the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Reform Act of 1996 (Clinger-Cohen), improving upon these existing requirements. Additionally, GISRA enacted in statute existing OMB IT security policies found in OMB Circular A-130 on IT management and OMB budget guidance in Circular A-11. As a result, GISRA both integrated and reinforced long-standing IT security requirements. GISRA also introduced new review and reporting requirements and defined a critical role for agency Inspectors General (IGs) to play in independently evaluating agency IT security. Agency Chief Information Officers (CIOs) and program officials are responsible for conducting annual IT security reviews of their programs and the systems that support their programs. Agency IGs must perform annual independent evaluations of the agency's IT security program and a subset of agency systems. The results of these reviews and evaluations are reported annually to OMB and are the basis of OMB's annual report to Congress.

In July 2002, OMB provided instructions for Federal agencies' reporting the results of their annual reviews and evaluations. Agencies' FY 2001 reports established a baseline of agency IT security status. The FY 2001 and FY 2002 reporting instructions are nearly identical and are closely aligned with the requirements listed in GISRA. Additionally, as part of the FY 2002 guidance, OMB, working with the agencies, took steps to provide the Congress and GAO with additional information from agency POA&Ms. As a result, the combination of the GISRA reporting requirements, OMB's reporting instructions, and agency plans of action and milestones (POA&Ms) have resulted in a substantial improvement of the accuracy and depth of information provided to Congress relating to IT security. In addition to IG evaluations, agencies are now providing the Congress with data from agency POA&Ms and agency performance against uniform measures.

Measuring Performance

The most significant difference in the FY 2002 reporting guidance compared to the FY 2001 was the introduction of government-wide IT security performance measures. Consistent with GAO's findings, measures were incorporated within the existing instructions, requiring agencies and IGs in some instances to report the results of their reviews against the measures. Through these performance measures, the Federal government has a clear picture for the first time of IT security status and progress. From agency responses, areas of progress as well as areas of problems are evident. As a result, the FY 2002 reports clearly identify Federal agency's FY 2002 status and identify both progress made from their FY 2001 benchmark as well as new and remaining weaknesses.

I am pleased to report to you today that the Federal government has made substantial improvements in securing its information and information systems. OMB's annual report to Congress will provide more details but I would like to provide you with some examples of progress. For example:

- In FY 2001, only 40% of Federal systems had up-to-date system security plans. In FY 2002, that percentage increased to 61%.
- Similarly, the number of Federal systems certified and accredited increased from 27% in FY 2001 to 47% in FY 2002.

Table 1 below provides additional information on the Federal government's progress and is a subset of what we expect to include in the annual OMB report.

Table 1. FY 2002 Government-wide IT Security Performance

Total Number of Systems		Percentage of systems assessed for risk and assigned a level of risk		Percentage of systems that have an up-to-date IT security plan		Percentage of systems authorized for processing following certification & accreditation		Percentage of systems with a contingency plan	
FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02	FY01	FY02
7282	7957	44%	64%	40%	61%	27%	47%	30%	53%

* Data provided from agencies' FY 2002 GISRA reports to OMB.

While these measures reveal in some cases over 50% performance improvement from the FY 2001 baseline and

confirm the value of the review and reporting process in place, they also identify the magnitude of work yet to be done. The Federal government is heading in the right direction but the numbers are still too low.

Agency GISRA reports and IT budget materials provide an update on IT security spending. Federal agencies plan to spend \$4.25B in FY 2003 on IT security, roughly 7% of the Federal government's overall IT budget, and a 57% increase from the \$2.7B identified in FY 2002. As FY 2002 was the first budget year in which IT security costs were reported, this increase is largely attributed to improved reporting as well as a general increase in IT security. From the FY 2004 IT budget materials, agencies plan to spend \$4.7B on IT security or 8% of the Federal government's overall IT budget of \$59B, representing an 11% increase from FY 2003.

The FY 2002 GISRA reports also identify a number of other positive outcomes: 1) More Departments are exercising greater oversight over their bureaus; 2) At many agencies, program officials, CIOs, and IGs are engaged and working together; 3) IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process; and 4) More agencies are using their POA&Ms as authoritative management tools to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected.

Six Common Government-wide IT Security Weaknesses From FY 2001

In the FY 2001 summary report to Congress, OMB identified six common government-wide weaknesses based on our review of agency and IG reports. A year later, progress is clearly evident across these six areas and while additional efforts are still warranted, the Federal government is heading in the right direction.

1. *Increasing agency senior management attention to IT security.* At the end of each fiscal year, agency heads now submit the security program review to OMB. The conditional approval or disapproval of agency IT security programs is directly communicated between the OMB Director and each agency head. In addition, OMB used the President's Management Agenda Scorecard to focus attention on serious IT security weaknesses. Through the scorecard, OMB and

senior agency officials monitor agency progress on a quarterly basis. As a result, senior executives at most agencies are paying greater attention to IT security.

2. *Development of IT security performance measures.* The absence of government-wide IT security performance measures was addressed in the FY 2002 reporting instructions. These high-level management performance measures assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific IT security requirements. Agencies reported the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. These measures are mandatory and help to ensure that accountability follows authority.

3. *Improving security education and awareness.* Through the Administration's "GoLearn" e-government initiative on establishing and delivering electronic training, IT security courses were available to all Federal agencies in late 2002. Initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers, and the general workforce. Additionally, NIST has developed and issued for review guidance to agencies on building an IT security awareness and training program.

4. *Increasing integration of security into capital planning and investment control.* OMB continues to aggressively address this issue through the budget process, to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Through this process agencies can demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. OMB also provided agencies guidance in determining IT security costs of their IT investments. As a result, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved IT security performance.

Agencies have made improvements in integrating security into new IT investments. However, significant problems remain in regards to ensuring security of legacy systems.

5. *Working toward ensuring that contractor services are adequately secure.* Through the Administration's Committee on Executive Branch Information Systems Security of the President's Critical Infrastructure Protection Board, an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. This issue is currently under review by the Federal Acquisition Regulatory Council to develop, for government-wide use a clause to ensure security is addressed as appropriate in contracts.

6. *Improving process of detecting, reporting, and sharing information on vulnerabilities.* Early response for the entire Federal community starts with detection of threats, vulnerabilities and attacks by individual agencies who report to incident response centers at the Department of Homeland Security (DHS), DOD, or elsewhere. While it is critical that agencies and their components report all incidents in a timely manner it is also essential that agencies actively install corrective patches for known vulnerabilities. To further assist agencies in doing so, the Federal Computer Incident Response Center (FedCIRC) awarded a contract on patch management. Through this work FedCIRC will be able to disseminate patches to all agencies more effectively. To date, 19 of the 24 Chief Financial Officer Act agencies have established patch authentication and distribution accounts. There are currently 176 active users in these agencies, and that number is increasing steadily as this new service continues to be implemented.

In addition, FedCIRC has implemented a 7X24 emergency notification process to rapidly alert agency CIOs to emerging cyber threats and critical vulnerabilities. CIOs are notified of specific actions needed to protect agency systems and agencies must then report to OMB on the implementation of the required countermeasures. The emergency notification and reporting process has been used three times since the beginning of the year - first for the Slammer Worm and then for the Sendmail and IIS vulnerabilities. As a result of these early alerts, agencies have been able to rapidly close vulnerabilities that otherwise might have been exploited. As FedCIRC and related organizations have moved to DHS, additional progress is being made on sharing information needed for Federal agencies to respond to vulnerabilities and cyber threats.

IT Security and E-government Initiatives

OMB's work on Expanding E-Government under the President's Management Agenda identifies IT security as a key issue. Two of the initiatives, E-Training and E-Authentication, provide significant opportunities for leveraging the Federal government's resources to improve IT security. The benefits of the E-Training initiative were identified above. Through the E-Authentication e-government initiative, the Administration deployed and tested a prototype e-Authentication capability in September. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls across government. The full capability is expected in September 2003.

Improvements in Critical Infrastructure Protection and Federal Incident Response

Experts agree that it is virtually impossible to ensure perfect security of IT systems. Therefore in addition to constant vigilance on IT security we require agencies to maintain business continuity plans. OMB directed all large agencies to undertake a Project Matrix review to ensure appropriate continuity of operations planning in case of an event that would impact IT infrastructure. Project Matrix was initially developed by the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce. As you know the CIAO and its functions were transferred to DHS. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector.

Coordination of the Federal government's cyber security and critical infrastructure protection efforts continues under the leadership of the new Homeland Security Council's (HSC) Special Assistant to the President for Critical Infrastructure Protection, and the Assistant Secretary for Infrastructure Protection at DHS (who is responsible for cybersecurity coordination within DHS), in partnership with OMB. OMB works with the HSC and DHS, and all Federal agencies to ensure that through IT security policy and management and budget processes, our critical

operations and assets are appropriately identified along with the resources necessary to secure them. We are also working with DHS to improve the Federal government's response to cyber attacks, and vulnerabilities. The integration of FedCIRC, the National Infrastructure Protection Center (NIPC), and the CIAO under one Department, partnering with the Science and Technology directorate on research and development needs, presents an opportunity for the Administration to strengthen government-wide processes for intrusion detection and response through maximizing and leveraging the important resources of these previously separate offices.

Continuing Efforts to Improve IT Security

Budgeting for IT Security

All Federal systems require security. To identify the appropriate security controls, agencies must first assess the risks to their information and systems. Security must be incorporated into the life-cycle of every IT investment. As part of the IT business case (Form 300) for major systems, agencies report on that risk as well as their compliance with security requirements, i.e., development of security plans and certification and accreditation. Failure to appropriately incorporate security in new and existing IT investment automatically requires it be scored as "at-risk". As a result, that system is not approved to proceed for the fiscal year in which the funds were requested until the security weaknesses are addressed. As of the submission of this report, there are approximately 700 systems in the FY 2004 budget, totaling nearly \$19 billion, at-risk either solely or in part due to IT security weaknesses. Additionally, many agencies are not adequately prioritizing their IT investments and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

Government-wide IT Security Milestones

OMB set targeted milestones for improvement for some of the critical IT security weaknesses and included them in the President's FY 2004 budget. Targets for improvement include:

- More agencies must establish and maintain an agency-wide process for developing and implementing program and system level plans. Plans of action and milestones must serve as an agency's authoritative management tool, to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected. By the end of 2003, all agencies shall have an adequate process in place.
- Many agencies find themselves faced with the same security weaknesses year after year. They lack system level security plans and certifications. Through the budget process, OMB will continue to assist agencies in prioritizing and reallocating funds to address these problems. By the end of 2003, 80 percent of Federal IT systems shall be certified and accredited.
- While agencies have made improvements in integrating security into new IT investments, significant problems remain in ensuring security of new and in particular, legacy systems. By the end of 2003, 80 percent of the Federal Government's FY 2004 major IT investments shall appropriately integrate security into the lifecycle of the investment.

Department-wide Plan of Action and Milestone Process

Clearly, the more reviews agencies and IGs conduct, the more weaknesses they will find. As a result agency and IG reports are identifying an increased number of IT security weaknesses. To ensure that appropriate and timely corrective actions are taken, OMB guidance directs Federal agencies to develop 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 prioritized, tracked, and corrected. These plans must be developed, implemented, and managed by the agency official who owns the program or system (program official or CIO depending on the system) where the weakness was found. System-level POA&Ms must also be tied directly to the budget request for the system through the IT business case. This is an important step that ties the justification for IT security funds to the budget process.

Expanding E-Government under the President's Management Agenda

To ensure successful remediation of security weaknesses throughout an agency, every agency must maintain a central process through the CIO's office to monitor agency compliance. OMB's draft FY 2003 guidance to agencies for reporting under FISMA will direct agency IGs to verify whether or not an agency has a process in place that meets criteria laid out in OMB guidance. OMB has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard. An IG approved agency-wide POA&M process is one of a number of milestones necessary for agencies to improve their status on the Expanding E-Government Scorecard.

IT Security Performance Measures

OMB will also incorporate the performance measures I discussed earlier into the quarterly POA&M reporting, coinciding with the Scorecard assessment. Agencies will report each quarter on their progress, by bureau, against those measures.

Conclusion

GISRA has clearly had a tremendous impact on the state of Federal IT security. The framework and processes in law and OMB policy have reinforced the importance of management, implementation, evaluation, and remediation to achieving real IT security progress. Due to the significant work of Federal agencies and IGs, along with the Congress and GAO, we are able to point to real advancement in closing the Federal government's IT security performance gaps. With all of that progress, we still have a long way to go to appropriately secure our information and systems. Many pervasive IT security weaknesses remain, leaving the Federal government with unacceptable risks. OMB will continue to work with agencies, Congress, and GAO to ensure that appropriate risk-based, and cost-effective IT security programs, policies, and procedures are in place to secure our operations and assets.