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 GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES

March 6, 2002

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss the lessons learned from implementation of the Government Information Security Reform Act (Security Act). Additionally, I would like to talk with you about the recent OMB report to Congress on Federal government information security reform, our findings in the report, and the next steps we are taking with agencies to improve IT security.

Before I get to the substance of my testimony, I need to make sure the Subcommittee understands that I do not serve in a confirmed position within the Office of Management and Budget (OMB). As a general policy, OMB does not usually send officials in non-confirmed political positions to testify before Congress. However, because of the importance of the issue and the fact that OMB does not yet have a Deputy Director for Management, the OMB Director decided it was in the best interest of the Administration to have me appear on his behalf as a witness for this hearing.

As you know, the President has given a high priority to the security of government assets including government information systems and the protection of our nation's critical information assets from cyber threats and physical attacks. We believe that protecting the information and information systems on which the Federal government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats.

Last October, the President issued Executive Order 13231,"Critical Infrastructure Protection in the Information Age." This Executive Order establishes the Critical Infrastructure Protection Board and creates a Chair who serves as the Special Advisor to the President for Cyberspace Security. This Board will promote greater coordination and consistency among the Federal agencies. The Board will oversee work to ensure that: Federal policies and processes are appropriate so that critical commercial and government IT assets are adequately secure; emergency preparedness communications are operating adequately; and government and industry work closely together to address increasing interconnections and shared risk. Richard Clarke serves as Chair of the Board and Special Advisor to the President for Cyberspace Security, and reports both to Governor Ridge on issues that affect homeland security and to National Security Advisor Condolezza Rice on issues that affect national security.

The President has made OMB a member of the Critical Infrastructure Protection Board. OMB's presence reflects our statutory role regarding the security of Federal information systems. Additionally, OMB chairs the Board's standing committee on Executive Branch Information Systems Security.

Government Information Security Reform

The Administration has been proactive in implementation of the Government Information Security Reform Act (Security Act). This includes expansion of its reporting requirements to include CIO and senior agency officials' input with IGs, and moving beyond simply reporting security weaknesses and instead focusing on agency work to remediate their security weaknesses. The basic push behind our continuing work is a strong focus on management implementation of security.

Senior Management Attention to Security

In January, OMB Director Mitch Daniels sent letters to the heads of agencies communicating our concerns regarding their FY01 security programs. The primary purpose of these letters was to capture senior management attention. In general, agency heads responded in writing with a commitment to resolve their past flaws. As follow-on from these letters, the OMB summary report, and agency

corrective action plans, OMB will soon meet with all 24 large agencies.

As you know, the President has charged Director Daniels with overseeing the implementation of his Management Agenda through the use of an Executive Branch Management Scorecard. This Scorecard tracks agency improvement in five government-wide problem areas and assigns a red, yellow, or green score. Under one of these areas, expanding electronic government, we are incorporating IT security as a core criteria. This means that if an agency does not meet the IT security criteria it will not achieve a green score regardless of their performance under the other e-gov criteria. Additionally, IT security is a key component of the other Management Agenda items.

OMB Guidance on Remediating Security Weaknesses

Last fall, OMB issued guidance to agencies on the development and submission of security plans to correct weaknesses. These plans require agencies to identify, assess, prioritize, allocate resources, and monitor the progress of corrective efforts for their security weaknesses. They are important because they bring a discipline to the process, are a valuable management and oversight tool, and make tracking progress much easier for all involved.

Additionally, Federal agencies are required to provide quarterly updates to OMB. The information provided to OMB in the initial plans of action and milestones (POA&Ms) were used during the FY03 budget process to prioritize agency funding for security and define remediation activities.

Successful implementation of corrective action plans that appropriately address all weaknesses will bring agencies a long way toward positive overall security performance, progress that we expect to document in next year's report to the Congress.

I would also like to point out that while we all tend to focus largely on the 24 Chief Financial Officers Act agencies, these action plans are also being developed by over 30 small and independent agencies, such as FDIC, SEC, and NEH. We plan on meeting with the small and independent agencies as well.

OMB Report to Congress – Findings and Next Steps

As you know, one of OMB's responsibilities under the Security Act is to submit annually a summary report to Congress summarizing the results of security evaluations conducted by agencies and reported to OMB. On February 13th, Director Daniels transmitted this report to Congress.

At this time I would like to recognize the tremendous amount of work of agency program officials, CIOs, IGs, and all of their staffs in conducting the reviews and evaluations. This was a large effort for all involved and the report illustrates this work as well as the ongoing efforts of agencies to remediate their weaknesses.

Additionally, the National Institute of Standards and Technology (NIST) continues to play a critical role in promoting IT security requirements among agencies. Among their activities they have recently issued security guidance on telework, security webservers, and cryptography. OMB policy requires that each agency's program shall implement policy standards and procedures, which are consistent with NIST guidance. Also, NIST has developed a security questionnaire, based on the Federal CIO Council and NIST Security Framework. This security questionnaire assists agencies in performing self-assessments of their IT systems. It is based primarily on NIST technical guidance and GAO's Federal Information System Controls Audit Manual and allows agencies to assess the management, operational, and technical controls of their systems. Indeed, most agencies used this document as the basis for conducting their annual reviews under the Security Act. We are currently working with NIST on the automation of this tool for agency use.

This report represents the first year of implementation of the Security Act. It is a valuable baseline that has recorded agency security performance. The findings in the report are based solely on work performed by agencies during the FY01 reporting period. Our report briefly describes recent Administration activities involving IT security -- namely the President's Executive Orders on Homeland Security and Cyber Security. The report discusses the steps taken by OMB and Federal agencies to implement the Security Act as well as additional efforts OMB and the agencies have taken to improve Federal information technology security.

From our assessment of agency performance under the Security Act, we have both validated our earlier positions on the problems with IT security and identified important lessons learned:

1. Security is primarily a management problem, not a technical or funding problem;

2. Increased security spending does not necessarily translate into increased security performance;

3. High quality IG audits are necessary. Prior to the Security Act IG involvement in IT security was largely through their work in financial management. IGs provide an important independent validation function; and

4. Agency employees with specific security responsibilities must have the authority to fulfill their responsibilities and be held accountable for their performance.

Our report also identifies six common government-wide security weaknesses we found in our review of agency submissions, along with activities underway by OMB and the agencies to resolve them. Where agencies are performing well, we identified their actions as examples of effective practices.

For the most part these weaknesses are not new or surprising. We, along with GAO, and agency IGs, have found them to be problems for at least six years. This time, the evaluation and reporting requirements of the Security Act have given OMB and Federal agencies an opportunity to develop a comprehensive cross government baseline of agency IT security performance that has not previously been available. As I mentioned earlier, OMB has taken steps to maximize this opportunity through additional guidance requiring agencies to develop and submit initial corrective action plans.

I will briefly discuss these weaknesses and the next steps the Administration is taking to assist agencies in resolving them.

1. Senior management attention. Senior leaders must consistently establish and maintain control over the security of the operations and assets for which they are

responsible. As the Security Act recognizes, security is a management function which must be embraced by each Federal agency and agency head.

Next Steps: OMB is working through the President's Management Council to promote sustained attention to security as part of OMB's work on the President's Management Agenda and the integration of security into the Scorecard that I spoke of earlier.

2. Measuring performance. Agencies must be able to evaluate the performance of officials charged with implementing specific requirements of the Security Act. To evaluate agency actions, OMB requested data in the FY01 Security Act reports that agencies measure job and program performance, i.e., how senior leaders evaluate whether responsible officials at all levels are doing their job. They must be able to evaluate the performance of officials charged with securing agency operations and assets. Virtually every agency response regarding performance implies that there is inadequate accountability for job and program performance related to IT security.

   Next Steps: OMB has drafted quantifiable management level performance measures for agencies to identify the performance gaps in their IT security work. Our guidance for last year's report required agencies to respond to 13 topic areas, which represented the requirements of the Security Act and OMB budget guidance. They range from questions on agency security training and incident response capabilities to the integration of security into their capital planning processes. Our FY02 guidance will still contain these questions, but will move beyond the baseline and focus on progress. We will require agencies to report the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. To ensure that accountability follows authority, the measures are organized according to the Federal employee responsible. These measures are mandatory and represent the minimum metrics against which agencies must track against to ensure performance and measure progress. We encourage agencies to develop additional measures that address their needs.

Additionally, NIST is developing technical security metrics that will assist agencies in measuring the security performance of their programs and systems and help them implement appropriate security controls to protect their programs and systems.

3. Security education and awareness. Agencies must improve security education and awareness. General users, IT professionals, and security professionals need to have the knowledge to do their jobs effectively prior to be held accountable.

   Next Steps: OMB and Federal agencies are now working through the new Critical Infrastructure Protection Board's education committee and the CIO Council's Workforce Committee to address this issue. Additionally, the CIO Council's Best Practices Committee is working with NIST through NIST's Federal Agency Security Practices website to identify and disseminate best practices involving security training. Finally, one of the Administration's electronic government initiatives is to establish and deliver electronic-training. This initiative will provide e-training on a number of mandatory topics, including security, for use by all Federal agencies, along with State and local governments.

4. Funding and integrating security into capital planning and investment control. Security must be built into and funded within each system and program through effective capital planning and investment control. As OMB has done for the past two years in budget guidance, Federal agencies were instructed to report on security funding to underscore this fundamental point. Systems that do not integrate security into their IT capital asset plans will not be funded.

   Next Steps: OMB continues to aggressively apply this approach 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. The IT investment justification and documentation process is key to sound program and financial management. Security must not be viewed differently. This process demonstrates explicitly how much agencies are spending on security and associates that spending with a given level of performance. Thereafter, Federal agencies will be far better equipped

to determine what funding is necessary to achieve improved performance. This is the security component of the business case.

5. Ensuring that contractor services are adequately secure. Agencies must ensure that contractor services are adequately secure as most Federal IT projects are developed and many operated by contractors. Therefore, IT contracts need to include adequate security requirements. Many agencies reported no security controls in contracts or no verification that contractors fulfill any requirements that may be in place.

   Next Steps: Under the guidance of the OMB-led security committee established by E.O. 13231, an issue group will develop recommendations, to include addressing how security is handled in contracts themselves. We are working with the Federal Acquisition Regulatory Council to develop for government-wide use a clause to ensure security is addressed as appropriate in contracts.

6. Detecting, reporting, and sharing information on vulnerabilities. Far too many agencies have virtually no meaningful system to test or monitor system activity and therefore are unable to detect intrusions, suspected intrusions, or virus infections. This places individual agency systems and operations at great risk since response depends on detection. Perhaps most significant, not detecting and reporting IT security problems could cause cascading harm. Our vastly inter-networked environment also means an environment of shared risk with the best security being only as strong as the weakest security.

   Early warning for the entire Federal community starts first with detection by individual agencies, not incident response centers at the FBI, GSA, DOD, or elsewhere. The latter can only know what is reported to them, reporting can only come from detection, and guidance for corrective action depends upon both. This need is thus not a technical one, but a management one. Additionally, it is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center and appropriate law enforcement authorities such as the FBI's National Infrastructure Protection Center as required by the Security Act.

Next Steps: GSA's Federal Computer Incident Response Center reports on a quarterly basis to OMB on the Federal government's status on IT security incidents. Additionally, under OMB and Critical Infrastructure Protection Board guidance, GSA is exploring methods to disseminate patches to all agencies more effectively. Additionally, I plan on issuing updated guidance to agencies on reporting to FedCIRC, stressing the necessity for accurate and timely reporting.

While not addressed in our report, we also found that agencies have not implemented a disciplined process for systems security planning, accreditation, and review. The first such review is comprehensive and complex, but subsequent ones are simply maintenance; NIST is completing its automation of their tool for agency use to conduct these reviews.

While OMB can and will continue to assist agencies with their efforts in addressing their security weaknesses, both the responsibility and ability to fix these weaknesses and others, ultimately lie with agencies. IGs, OMB, and GAO cannot do it for them.

Additional OMB Actions

Finally, I would like to provide you with more detail on three other items that we continue to work on.

1. OMB Security Committee. In our report we mentioned the formation of a security committee on Executive Branch Information Systems Security. OMB will chair this standing committee under the President's Critical Infrastructure Protection Board. The CIP Board was created by the President in Executive Order 13231,"Critical Infrastructure Protection in the Information Age." This Executive Order establishes the Critical Infrastructure Protection Board and creates a Chair who serves as the Special Advisor to the President for Cyberspace Security. The goal of the Board is to promote greater coordination and consistency among the Federal agencies. Members of the committee will be representatives from all the key communities in the Federal government that have a role in IT security. This includes CIOs, CFOs, PEs, IGs, agency program officials, agency security managers, and

HR folks. Most of the Committee's work will be performed by individual issue groups. These issue groups will form to address a discrete issue such as security and acquisition as designated by the Committee (including issues referred by other organizations, committees, and individual agencies). Upon completion of an issue, the issue group will dissolve. The work of the Committee will occur under existing policy and guidance setting authorities. Neither the Committee nor the issue groups have any policy or guidance setting authority and thus shall not issue guidance or other documents.

2. IT Security and the Budget. OMB will continue to engage the agencies in a variety of ways to address the problems that have been identified, continuing to emphasize both the responsibilities and performance of agency employees in addition to accountability for exercising those responsibilities and consequences for poor performance. We will continue to rely on traditional budget and management processes to ensure that IT security needs are being addressed. OMB has made it a policy to stop funding projects that do not adequately address security requirements and neglect to document how security planning and funding is integrated into the project's life cycle.

   To ensure that security is addressed throughout the budget process OMB established the following four criteria:

   -- Agencies must report security costs for each major and significant IT investment. In the long run, it will greatly help agencies demonstrate explicitly how much they are spending on security and associates that spending with a given level of performance. Thereafter, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved performance. This is the security component of the business case. We do this to ensure that security is included and funded for each IT investment throughout the life of the investment. We do not use security funding as an indicator of good security. It is an indicator of good security management -- that the agency has integrated security and views security as a

critical component of the entire investment and not as an add-on.

-- Agencies must document in their business cases that adequate security controls have been incorporated into the life cycle planning and funding of each IT investment.

-- Agency security reports and corrective action plans are presumed to reflect the agency's security priorities and thus will be a central tool for OMB in prioritizing funding for systems.

-- Agencies must tie their corrective action plans for a system directly to the business case for that IT investment.

Additionally, we developed through the budget process, a process for tracking projects that are at risk due to poor business cases. We are currently tracking nearly 400 major IT projects which amount to approximately $10B of both the Federal government's $48B FY02 IT spending and $52B FY03 IT spending. Of the 400 projects roughly half are at risk in part to poor demonstration of security planning, procedures, and controls. Poor security in projects amount to just over $6B (full IT investment costs) of the $10B at risk. We are working with agencies to address these concerns and many of them are currently revising their plans to address the problems.

3. Enterprise Architecture and Project Matrix. The development of a government-wide enterprise architecture is a central part of the Administration's electronic government efforts. Establishment of an architecture for the Federal government will greatly facilitate information sharing based on the lines of business of each agency. Additionally, this architecture will identify redundant capabilities and provide ample opportunities to increase efficiencies while reducing costs, and duplicative programs. Accordingly, OMB will also be able to better prioritize and fund the Federal government's security needs.

To more clearly identify and prioritize the security needs for government assets, OMB will direct all large agencies to undertake a Project Matrix review. Project

Matrix was developed by the Critical Infrastructure Assurance Office of the Department of Commerce. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector. This is largely a vertical view of agency functions. To ensure that all critical government processes and assets have been identified, once reviews have been completed at each large agency, OMB will identify cross-government activities and lines of business for Matrix reviews. In this way OMB will have identified both vertically and horizontally the critical operations and assets of the Federal government's critical enterprise architecture and its relationship beyond government.

Conclusion

In discharging OMB responsibilities under the Security Act, OMB has communicated with the appropriate agency heads to impress upon them that true improvements in security performance comes not due to external oversight from OMB, IGs, the General Accounting Office (GAO), or Congressional committees, but from within – holding agency employees, including CIOs and program officials, accountable for fulfilling their responsibilities. I cannot stress this point enough – Security is the responsibility of every employee in the agency. There must be consequences for inadequate performance. OMB has also underscored the essential companion to accountability -- the need for clear and unambiguous authority to exercise responsibilities.

The first year of the Security Act has brought us all a better and more detailed understanding of the Federal government's IT security status than ever before. The reporting requirements of the Security Act have afforded agencies, IGs, GAO, OMB, and Congress the ability to capture a performance baseline. This baseline clearly illustrates significant and pervasive security weaknesses across every department and agency. We have considerable problems in IT security that requires serious attention. Now that we are better informed of our security weaknesses, and agencies have developed plans on how to remediate those weaknesses, the next step is continuing the implementation of those plans and determine our success through measuring performance.