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
November 9, 2001

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss the Administration's efforts in the areas of computer security. We know that our government and our nation rely increasingly on computer systems to support nearly every critical governmental and business function.

Government and industry are now more interconnected than ever, operating in a shared risk environment, with our interdependence growing daily. The integrity and availability of our systems and, where appropriate, the confidentiality and privacy of information in those systems are today more important than ever. The value of computer and telecommunications systems and the vital information they process and transport became even more apparent in the wake of the tragic events of September 11.

I would like to commend you and the Committee for your past and current efforts to shine the spotlight on Federal agency security performance. I believe that only by keeping the pressure on will improved performance be achieved and sustained.

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, in this case, because 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.

Setting the Context

The President has given a high priority to security of government assets including government information systems and to the protection of our nation's critical information assets. In addition to the real risk to our physical well being, he understands the growing risks that our nation faces from cyber threats and of course the risks to our cyber assets that physical attacks can bring.

At the same time we know that interconnected computer systems are necessary for the provision of essential national services. Government and industry face the same risks and must work in close partnership to mitigate those risks. Indeed, this risk is also shared globally.

The President has taken a number of steps to address these risks. First, on October 8, 2001, the President signed Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council" which provides for the implementation of a comprehensive national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats and attacks within the United States. As you know, the President appointed Governor Tom Ridge to head this office. The Governor and his staff are working hard to set the framework for this complex undertaking and the President recently convened the Homeland Security Council to help this process.

To work with Governor Ridge on issues related specifically to the topic of today's hearing -- the security of information systems -- the President appointed Richard Clarke as the Special Advisor to the President for Cyberspace Security. Mr. Clarke will be leading the Administration's cyberspace security efforts under the guidelines established in Executive Order 13231,"Critical Infrastructure Protection in the Information Age." Under this executive order, Mr. Clarke will chair the Critical Infrastructure Protection Board to promote greater coordination and consistency among the Federal agencies and ensure that Federal policies and processes are adequate to ensure information technology assets are adequately secure, that emergency preparedness communications are operating adequately, and that government and industry work closely together to address their ever increasing interconnections and shared risk.

The President has made OMB a member of both the Homeland Security Council and the Critical Infrastructure Protection Board to help identify resource shortfalls and duplication and ensure that funding requests are included in the President's budget as necessary and properly managed when appropriated by Congress.

OMB's presence on both organizations also reflects OMB's statutory role regarding the security of Federal information systems.

Among the issues that the Office of Homeland Security and the Critical Infrastructure Protection Board will focus on is the relationship between the government's programs for security, critical infrastructure protection, and continuity of government operations. In most respects these are related and complementary programs and effective implementation of one program helps promote effective implementation of the other two. At the same time, we want to remove any duplication of effort and find any wasteful expenditure of scarce resources so that collectively these programs can operate more effectively and be funded adequately.

The Legal Framework for Government Computer Security

In 1998 the Government Paperwork Elimination Act (GPEA) addressed OMB and agency responsibilities for conducting business in an electronic environment. The authors of GPEA had the foresight to recognize that improved government performance demands an ability to broadly accept authenticated electronic business transactions. Fulfilling this goal is essential to achieving the President's Management Agenda. We are now reviewing updated plans from the agencies to evaluate whether they are on track to meet the October 2003 GPEA deadline.

Last year, through passage of the Government Information Security Reform Act of 2000 (Security Act), Congress strengthened an already sound legal framework for the Executive branch to address computer security needs.

The Security Act amends the Paperwork Reduction Act of 1995 (PRA) by adding a new subchapter on Information Security and builds upon the Computer Security Act of 1987 and the Information Technology Reform Act of 1996 (Clinger-Cohen). Like the PRA itself and Clinger-Cohen, the Security Act binds agency security programs and practices to their overall program and information resource management and capital planning and budget processes.

The Security Act divides security programs into three basic components -- management, implementation, and evaluation.

-- For management, it recognizes that while security has a technical component, it is at its core, an essential management function.

-- For implementation, it recognizes that program officials (not security officers or CIOs) are

ultimately responsible for ensuring that security is integrated and funded within their programs and tied to the program goals.

Thus the Security Act highlights the reality that when security funding and implementation are separated from the operational program, program officials and users begin to ignore it. Separation sends the incorrect signal that it is not a program responsibility.

CIOs also have a significant role. They must take an agency-wide strategic view of implementation and ensure that the security of each program is appropriately consistent and integrated into the agency's overall program and enterprise architecture.

-- For evaluation, the Security Act requires program officials and CIOs to annually look at what they have done and what they believe remains to be done and for IGs to verify it.

OMB's Security Role and Current Activities

Working within the above legal framework, OMB's goal is to continuously improve Federal agency security programs. Our guidance:

-- ensures that agency senior managers devote greater attention to security;

-- requires agencies to tie security to their capital planning and investment control process and to their budgets as required by the Clinger-Cohen Act, the Security Act, and OMB policy;

-- helps agencies achieve consensus and get user buy-in when initially establishing security controls and processes to ensure that they enable and do not unnecessarily impede business operations;

-- requires that security is part of agency program management decision making -- to connect the dots from security to mission; and

-- makes adequate security a condition for the funding of each capital asset by requiring that security controls and their costs be explicitly identified in the life cycle planning for each system and program.

As you may have discerned from the agency security report submissions, the agencies have reported that for FY 2002 they were investing approximately $2.7 billion for security and critical infrastructure protection. This is from a total information technology budget of about $45 billion. But a high dollar figure says little about how effective security might be, so we are working hard to ensure that these resources are applied wisely for both security and information technology in general.

To ensure that security is addressed both in the apportionment of FY 2002 agency funding and in their FY 2003 budget requests, OMB has established the following four criteria:

-- Agencies must report security costs for each major and significant IT systems. Systems that fail to document security costs will not be funded.

-- Agencies must document in their capital asset plans that adequate security controls have been incorporated into the life cycle planning and funding of each system.

-- 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 capital asset plan for that system.

Government Information Security Reform Act Reporting

In September we began receiving the annual reports, required by the Security Act, from agencies. We are reviewing them now; because we know that there will be much consultation with the agencies regarding their submissions, it is too early to provide any specific findings regarding any particular agencies. We have provided you with the raw agency executive summaries and trust you find them useful, as you know they represent but one piece of the overall puzzle we are trying to assemble. Later, I will provide you some broad observations, but first I want to discuss our process and how we have gone significantly further than the law requires insofar as reporting and follow up are concerned.

As you know, the Security Act's reporting requirement is relatively narrow, i.e., each agency Inspector General (IG) must perform an annual independent evaluation of the agency security program, the agencies then send these to OMB, and we are to prepare a summary report to Congress.

Because security is a high priority for this Administration, we have expanded the Security Act's limited requirement. OMB first issued guidance on implementing the Security Act in January. This guidance clarified the roles and responsibilities of CIOs, program officials, IGs, and OMB responsibilities. Additionally, the guidance required agencies to prepare an executive summary consisting of two components, an IG and a CIO part, based on the results of their respective reviews.

Follow-up OMB guidance issued in June contained detailed instructions to agencies on how to report their results in the executive summaries. These executive summaries will serve as the basis for the OMB annual report to Congress. We have also required that agencies send to us sufficient documentation that supports their findings in the executive summary (the Security Act requires agencies to prepare reviews but not report them).

To ensure that this reporting does not devolve into a bureaucratic paper drill, we are also requiring that agencies produce for their own use and send to us copies of corrective plans of action and milestones for each weakness found by an IG evaluation, a program review, or any other review conducted throughout the year, including a GAO audit. OMB issued specific guidance for preparing and submitting these corrective action plans and provided a template to assist agencies in developing them. These plans are not just important to us, but to the agencies and IGs as well. They bring a discipline to the process and make tracking progress much easier for all involved. We will also seek brief quarterly certifications that corrective actions are on track.

We haven't stopped there. We are requiring that each of the agency program reviews (which should also include individual system reviews) and plans of action are tied to the budget process through the corresponding capital asset plan and justification submitted with the agencies' budget. In this way, we ensure that funding requirements for correcting the weaknesses identified in the plan of action are accounted for in the agency's funding for an asset. As I said earlier, unless security is incorporated into and funded as part of each investment, the investment itself isn't funded.

Finally, we intend to use the security reports from the agencies, information we have gathered from meetings with the agencies on integrating security into their capital planning processes, their budget submissions, and other sources to determine whether OMB must take steps to assist agencies in quickly correcting their most serious weaknesses.

Overview of Agency Annual Security Reports

In their security reports, agencies reported $2.7 billion in security costs for FY 2002. Despite this sizable investment and the fact that law and long-standing OMB policy give agencies extensive flexibility in implementing security in a way that comports with their operational realities, there still remain significant security concerns across the government. We do not believe that, again given the large total amount already being spent on security, that simply adding more money will solve the problems. Such an approach has not worked for IT in general -- it shifts attention away from effective management and investment of existing resources – and will not work for IT security.

Generally, from agency security reports, especially the work performed by the Inspectors General, we have found across the 24 CIO agencies that the most common problems involve inadequate compliance with existing OMB security policies and failure to follow implementing guidance for the Security Act. From our preliminary findings agencies must:

-- Do a much better job testing and evaluating basic security controls;

-- Improve the ongoing maintenance of system security;

-- Greatly improve employee training and awareness programs;

-- Do a better job at integrating security into the capital planning and investment control and budget processes to develop a better understanding of security costs and ensure that security is in the program planning mainstream;

-- Recognize the greatly increased risk of interconnection;

-- Ensure that every system supporting operations and assets are reviewed annually as part of a program review; and

-- Pick the low hanging fruit by installing readily available patches for commonly known vulnerabilities. This is a chronic problem identified by GAO, IGs, and most any security program review. It is also commonly reported from FedCIRC and others as the cause of some 90% of successful attacks on agency.

Recognizing that this is the first year for these reports, we have to expect incompleteness and inconsistency, but we will work with the agencies to ensure that any incomplete submissions are corrected and that each agency fulfills their security

responsibilities and meets the specific requirements of the Security Act and OMB guidance.

Security and Electronic Government

We have also taken steps to ensure security is a key component of other OMB activities. The Administration's E-gov Task Force identified and the President's Management Council approved 23 cross-agency e-gov initiatives. OMB, working with agencies, will refocus resources to assure that IT facilitates agency administrative efficiencies, and most importantly, maximizes citizen access. In the process of making government easier, quicker, cheaper, and more responsive we must also make sure that government and its information and services are adequately secure.

All of the e-gov initiatives must address security. In addition to a risk management plan, agencies must demonstrate for each initiative that security for the initiative has been assessed, appropriate security controls identified, and that the agency has a process in place to maintain effective security for the project over its life cycle. In addition, three of the e-gov initiatives specifically deal with security issues:

-- E-authentication: Ensuring that parties to a transaction are authorized to participate and ensuring the integrity of the transaction.

-- Wireless Networks: Ensuring effective and interoperable communications between public safety officials throughout all levels of government, before, during, and after their response to a variety of events, such as natural and technological disasters, terrorist actions, and criminal activities, as well as to conduct other life-saving activities such as search and rescue operations.

-- Disaster Assistance and Crisis Response: Providing a one-stop portal containing information from all public and private organizations involved in disaster preparedness, response, and recovery. It will address the consequences of a disaster whether natural or man-made, technical or physical.

Security, the Government-wide Architecture, and Project Matrix

As a central part of our e-gov efforts we are developing a government-wide enterprise architecture. 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, we will also be able to better prioritize and fund our security needs.

A significant piece of this effort is the identification of key critical assets. Unlike the larger general security program, identifying critical assets and their interrelationships is especially complex and time consuming. The Critical Infrastructure Assurance Office of the Department of Commerce has developed a critical asset identification program known as Project Matrix. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships within the agency and beyond -- the enterprise architecture. Project Matrix reviews have been conducted or have begun at nine large Federal agencies. OMB is directing most remaining large agencies to reallocate FY 2002 funds for a Matrix review. 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 we will have identified both vertically and horizontally the critical operations and assets of the government and their relationships beyond government -- the government's critical enterprise architecture.

Conclusion

The security problems found throughout the agency reports are not new. We have established a focused, cross-agency approach to address this serious issue. Building on the framework established in the Security Act, we are requiring agencies to document their work in corrective action plans to ensure that security problems are prioritized and resolved in a timely manner. Additionally, we have taken steps to further integrate these security activities into the budget process. Clearly, sustained senior management attention at the agencies is essential to ensure the success of these efforts.

We plan to engage the agencies in a variety of ways to address the problems that have been identified, we will be emphasizing both the responsibilities and performance of agency employees in addition to accountability for exercising those responsibilities and consequences for poor performance.

We are going to stop funding for any project that does not adequately address security requirements and neglects to document how security planning and funding is integrated into the life cycle of the project.

At the same time we are going to focus on achieving sustained senior management attention at the agencies. This has been a chronic problem that we, GAO and others have found over the years to be the underlying cause of poor security performance. Indeed GAO's 1998 Executive Guide to Information Security Management identified senior management attention as a key to security success at leading organizations.

In discharging our responsibilities under the Security Act, the Director will be communicating with the appropriate agency heads to impress upon them that true improvements in security performance comes not from external oversight from OMB, IGs, GAO, or Congressional Committees, but from within – holding agency employees, including CIOs and program officials, accountable for fulfilling their responsibilities under the Security Act. There must be consequences for inadequate performance. We will also underscore an essential companion to that accountability -- the clear and unambiguous authority to exercise the responsibilities.

Despite the security challenges we face, we are not delaying our aggressive move towards accomplishing the President's Management Agenda including using secure information technology to make government more effective, responsive, and citizen centric. We can and will accomplish our goals.

I want to thank you and the Committee for your help and continued focus on this important area. It is vital that we all work together to maintain this as a priority issue and thus promote a more secure government.