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 AND
THE SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY
U.S. HOUSE OF REPRESENTATIVES

May 2, 2002

Good morning Mr. Chairman and members of the Committee. Thank you for inviting me here today to discuss the Federal information systems security and the Federal Information Security Management Act. I will discuss these in the context of the current state of Federal security and our vision for the future.

Before I get into the substance of my testimony, I need to make sure that 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 confirmed 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.

I know you would like to hear today about our specific views on the Federal Information Security Management Act. While we at OMB and other Administration officials have discussed components of the Act with your staff, we are still developing an Administration position on the bill. We look forward to working with you as the bill moves through the legislative process. We are also working with your Senate colleagues on S.803 the "Electronic Government Act of 2002." As you know that bill simply reauthorizes the Government Information Security Reform Act (Security Act) by lifting the November 2002 sunset date on the statute.

As you know, the President has given a high priority to the security of government assets as well as to improving the overall management performance of Executive agencies. These priorities are interrelated. As I discussed this past March before the Committee, our review of agency security programs found that most security problems within the government are fundamentally management issues. We are tracking progress on both issues through the use of the Executive Branch Scorecard for the President's Management Agenda. This Scorecard tracks agency improvement in five government-wide issue areas and assigns a red, yellow, or green score. One of the five areas, expanding electronic government, directly incorporates security. This means that if an agency does not meet the IT security criterion it will not achieve a green score regardless of their performance under the other e-gov criteria.

Vision for Federal Security

Our vision for Federal government security is an order of magnitude improvement to support government programs and enable a successful expansion of e-government. Security -- providing the necessary degree of confidentiality, availability, integrity, reliability for data and systems and ensuring the authenticity of transactions -- is integral to successful e-government.

The "As Is" State of Federal Security

As OMB reported in our February 13, 2001, security benchmark report to Congress on Government Information Security Reform, the "as is" state of security across the Federal enterprise is poor. We reported on six common fundamental government-wide weaknesses, as well as agency specific gaps. These weaknesses are pervasive and many exist within both the national security community and the larger non-national security community of Federal agencies.

We found that agencies must greatly increase their degree of senior management attention, measure the performance of officials charged with security responsibilities, improve security education and awareness, fully integrate security into the capital planning and investment control process and enterprise architecture, ensure that contractor services are adequately secure, and

improve the ability to detect, report, and share information on incidents and vulnerabilities.

Through the use of OMB's authorities under existing law, most particularly the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Government Information Security Reform Act of 2000, we are using the capital planning and investment control and the budget process to drive performance improvements in all of the problem areas that we identified.

The "To Be" State of Federal Security

The "to be" state of Federal security is one of active measures to anticipate future threats and vulnerabilities, preempt them where we can, prepare and defend against them where preemption is not possible, and survive attacks when defenses fail. Such a state is some years off however and a number of fundamental management and program reforms are needed to support the consistent and increased use of automated tools to manage threats. Many of these reforms are envisioned in the e-government initiatives and are outside of the control of security programs. Particularly, we need to complete the development of agency and government-wide architectures within which business processes have been unified and simplified and unnecessary duplication removed. This will not only promote common ways to conduct government business, it will permit common protection regimes and simplified security approaches.

The "to be" state also requires much in the way of using and improving existing automated security tools and developing new ones that reduce the need for human intervention and reduce human error and resource requirements. These are force multipliers for security and will assist in addressing some of the technology induced security problems. They will not however address all security problems as security is ultimately a management issue and technology demands the management commitment to sustain the use of technology.

The "to be" state will also include centralized and simplified ways to train Federal employees and to automate the retrieval and installation of patches and hot fixes for technology problems much in the way individual systems owners can do today. Again however, such a state depends

first upon a more uniform business and technical architecture than currently exists.

Improved Incident Handling and Reporting and Cross-Government Data Sharing

The "to be" state of anticipating threats will also require something that is woefully lacking today, in depth threat analysis. Today's analysis products consist largely of consolidated reports of what is happening or what has already occurred. That is not good enough. We must improve the development, quality, and wide distribution of threat analysis performed by government and industry leaders. Only in this way will agencies be capable of anticipating and preempting threats and vulnerabilities versus reacting to incidents after they have begun. This will not occur overnight and wisely spent research and development funding will be crucial to success.

Near and Mid-Term Steps to Achieve the "To Be" State

Security Improvements at the Agency Level

We are building towards the "to be" state and within 18 months, we will demonstrably improve the performance and results of agency security programs through:

1) Completing the integration of security into the agency's enterprise architecture and capital planning and investments control process to ensure that agencies make better decisions when investing in information technology and that the adequate level of business enabling and cost effective security is built into and funded over the life cycle of all IT projects,
2) Improving security management at each agency and integrating it into the agency's overall management structure and processes thus permitting each agency to move from today's reactive security posture to one of continuous risk management including the use of automated tools to actively look for, anticipate, and counteract threats and vulnerabilities before they are employed or exploited,
3) Ensuring that each department and agency maintains a department-wide program which actively oversees and verifies improved security performance in all components,

4) Measuring agency and component security performance and progress through reporting requirements under the Government Information Security Reform Act and through use of the President's Management Agenda Scorecard, and
5) Using security performance measurements to identify performance gaps and set priorities within each agency, inform agency and OMB budget decisions, and assist in preparing the President's budget.

Security Improvements at the Federal Enterprise Level

We are also seeking to improve the federal government's internal effectiveness and efficiency by simplifying and unifying security to facilitate programs and interoperability among Federal agencies and with State and local governments, industry, academia, and the public.

Many agencies perform similar business operations, especially internal management operations. The security requirements for such operations are also similar. Potential values in unifying and simplifying security include reduction or stabilization of staff resources, operational effectiveness, and stabilized spending.

Using an e-government-like approach, we are identifying opportunities for reducing or eliminating unnecessary duplication of security effort among agencies, making certain practices more uniform, and consolidating programs and operations to increase performance while reducing costs. Among the candidates for consolidation or greater uniformity are:

1) Consolidating security curriculum development as well as the actual conduct of training, education, and awareness for Federal employees. This will reduce unnecessary duplication of individual agency training infrastructures,
2) Improving incident handling, information sharing, and software patch identification and distribution. Centralizing access to and implementation of security patches will be more cost effective and improve agency performance,
3) Improving methods for grading or designating the level of risk to agency operations and assets. Developing a uniform methodology for use by all agencies will promote a common understanding of risk

levels and facilitate interoperability and information sharing,

4) Assigning core security requirements for operations and assets at the same risk level. Many agency operations and systems are the same and so to are many of their security requirements,
5) Unifying and simplifying requirements for and implementation of contingency planning and continuity of operations for agency communications and data networks. All critical Federal operations require the capability to continue or quickly restore functions and the methods to do so and implementation should be consistent across the Federal enterprise,
6) Improving the acquisition of products and services. In this two part effort, we will ensure that as law requires, all outsourced Federal operations be secured in the same manner as in-house operations and leverage the combined purchasing power of the Federal government and its industry partners to provide an incentive for industry to develop more reliable and secure products for all consumers.

A Cautionary Note – For Security, One Size Does Not Fit All

While many security requirements within the government are similar, many are distinctly different. We must be careful and resist overly simplistic attempts to standardize management, operational, and technical security controls in a non-standardized world. Thus, security controls must be built to the specifications of the program, not vice versa.

Attempting a one size fits all security approach is the fundamental flaw in past and some present attempts to standardize security. This is especially true when we try to apply national security requirements to non-national security programs where the vast majority of programs demand interoperability with industry, academia, and the public. Certainly, many of the needs are similar, and we must share approaches where we can, but the differences are far greater and require greater flexibility.

We have many historic examples of what happens when security is employed that is incompatible with the business needs. These examples exist within both the national security community and the non-national security community.

Some of these are contemporary history, playing out before us today.

Draconian and costly new security controls are often developed and employed following a significant security breach while an organization still feels the sting of embarrassment. These controls may work for a while, but are soon recognized as such an impediment to the mission that restrictions are relaxed, waived, or worse, ignored and worked around. As the sting subsides, further relaxation and waivers occur and the organization often finds itself back to the beginning point – no security. The cycle repeats itself.

Our approach is to fully integrate risk-based and cost effective security into the business processes and agency decision-making and thus avoid wild swings in security performance.

A Continued Strong Role for NIST is Essential to Improving Government-wide Security

NIST continues to play a critical role in supporting OMB and in assisting the agencies improve their security performance by developing new and updated technical guidance and detailed procedural security guidelines. They have recently either finalized or issued for public comment guidance on risks involving broadband telework and securing web and electronic mail servers. They will soon release for comment guidance regarding the security of wireless networks – an increasingly popular technology whose use is not without risk. Soon, NIST will release the automated version of their security self-assessment tool that most agencies used last year (including some within the national security community) to conduct their security reviews for reporting to OMB.

Among the most valuable of NIST's many abilities is fostering an open process (working with agencies, industry, and academia) that ensures that risks are objectively assessed and security guidance includes an understanding of the real world needs of agency program operations.

Working with NIST, one of the ways OMB is assisting the agencies is through a review of all current security policies, standards, guidance, and guidelines to identify gaps in coverage and effectiveness. Where gaps are found

we will close them, where confusion or uncertainty exists, we will clarify and simplify, and where more detail is necessary, we will provide it.

We began this gap analysis in April using the OMB-chaired Committee on Executive Branch Information Systems Security. This committee, which was established by E.O. 13231, "Critical Infrastructure Protection in the Information Age," is comprised of Chief Information Officers, Chief Financial Officers, Procurement Executives, Inspectors General, operational program officials (business lines), budget officials, human resource officials, security program managers, representatives from the national security community, law enforcement officials, and small agency representatives – all communities affected by security.

The policy gap analysis, as with all issues reviewed by this committee, will assess the performance benefits and costs of current or proposed policies in terms of whether they specifically: 1) are consistent with the President's Management Agenda and electronic government initiatives; 2) assist or impede agency business operations including introducing unintended negative consequences to program operations; 3) are workable for small agencies; 4) complicate or simplify interoperability across agencies, with industry, and other organizations; 5) complicate or simplify implementation and compliance; 6) complicate or simplify procurement and acquisition decisions; 7) increase or reduce privacy; 8) assist or impede Homeland Security and law enforcement efforts.

Federal Enterprise Architecture and Inter-Relationships

To ensure complete and adequate security coverage, we are also identifying within the individual agencies, among multiple agencies, and across the government enterprise and various lines of government business, the key operations and assets of the government and their inter-relationships. This will permit us to better identify security needs including contingency planning for those key lines of government business. It will also help us eliminate inconsistent security approaches across interrelated operations -- identifying the vault door on a shack.

Through the development of agency enterprise architectures and the use of Project Matrix we are

collecting this information now. While the current process captures much in the way of cross-organizational relationships, we have also allocated resources for a horizontal, cross government review by business line to identify any gaps in the agency-by-agency review. As part of this process, through the use of simulation models, we will evaluate the impact of threats on cross agency processes including continuity of business operations and data sharing.

Future Security Reporting Will Drive Performance Improvements, Not Simply Tally Numbers

As GAO, OMB and others recognize, today's information technology world demands that each agency employ a continuing process of risk management that keeps pace with the rapidly evolving threats and vulnerabilities. So too, OMB's oversight process must keep up with the changes in the status of agency programs.

Last year, as the Security Act required, we collected and provided to Congress a retrospective look at the state of each agency's security program -- a security baseline. This year we will collect much of the same data and will compare it to last year's baseline. The conventional view is that the comparison should show that security weaknesses have been reduced and no new ones have cropped up. But that is the old way of thinking -- identify last year's problems and wait until next year to see if the number has gone down.

This spring we are discussing with each of the large agencies the quality of last year's reporting and their plans to correct weaknesses identified in those reports. We have emphasized that we expect that the number of reported weaknesses to increase as they improve the quality of their self-assessment programs and reporting. More identified weaknesses is not necessarily a reflection of poor performance -- the more you look, the more you find - and OMB will not penalize agencies for finding more problems, provided of course they are taking appropriate measures to correct them in a timely manner and avoid recurrence.

OMB and NIST are also meeting with small and independent agencies either individually or collectively to ensure that they understand their responsibilities and are

taking steps to fulfill them. We will look for ways that they can partner with each other or work with larger agencies to assist them in achieving security performance improvements.

Reaching the "to be" state I described earlier demands digging more deeply and more often into program and systems to find and fix problems before they are exploited or an inspector finds them. Thus we are using the agency corrective action plans to drive this continuing process and are a key element for OMB oversight.

These corrective action plans must be the authoritative agency management tool to identify and manage the closing of agency security performance gaps. They must reflect all security weaknesses within an agency including its components and effective plans are iterative and do not have a specific beginning or end point. As old problems are corrected, they are removed. As new ones are found, they are added on.

What does a good plan look like? In addition to being a living document that catalogs problems as they are found, for a large agency, a comprehensive plan will consist of scores or hundreds of pages comprising hundreds or thousands of weaknesses. These weaknesses vary in detail from broad headquarters program level issues to minute technical problems within individual systems located in remote field activities. Such a plan would also include the names of agency employees that are being held accountable for correcting individual security weaknesses.

OMB's guidance prescribes a level of detail that enables agency management and OMB to manage and oversee security and inform the budget process. To meet OMB requirements, agency plans must include subjective and predecisional data to support a free and frank discussion between each agency and OMB. This data includes the agency's views of future resource requirements, the proposed source of those resources, and relative priorities for corrective actions and resources. In developing the President's budget, OMB must then view the security data together with agency budget submissions in the larger context of all government programs and priorities. Inaccurate assumptions invariably result from viewing predecisional data out of the larger context.

Many agencies have recognized that effective security management across a large organization requires that they collect and manage even more data than the minimum requested by OMB and they have or are developing complex databases that track this data.

Congress has an Essential Oversight Role

Congress and GAO are important strategic partners in our efforts to actively oversee government-wide security performance. We must all work together to move from the "as is" state to the "to be" state.

OMB agrees that some, perhaps most, of the data in the agencies' corrective action plans should be made available to Congress and we are modifying our guidance to the agencies to accommodate that goal.

OMB agrees that Congress has an important oversight role and will work toward an acceptable solution as quickly as possible. The challenge at this point involves identifying the proper level of detail, how to cull it from the predecisional data with which it is intertwined, and setting a reasonable schedule to provide it. We are addressing Congressional access needs in our guidance for the next agency submission of full corrective action plans next Fall.

Conclusion

As I told the Committee last March, we have found the current state of government security to be poor. We have identified about 200 agency information technology projects that are at risk due to poor security and there are probably as many more that could be on the list. Our goal is to find ways to assist the agencies in bringing them up to an acceptable level of performance.

We have developed a strategy to measure program performance and drive improvements by an order of magnitude. Some of what is needed involves technology, but much more involves integrating security into project development and management decision making. At this point in time, new standards or technologies will have little impact on improving security performance unless we first address and correct management weaknesses.