

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 19, 2002

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. As you know, year two of the Government Information Security Reform Act (Security Act) came to a close with the submission of agency and Inspector General reports in September. For the purposes of today's hearing, I will provide the Committee with OMB's initial analysis of the Federal government's IT security progress in fiscal year 2002.

Before I begin, I would like to first acknowledge the significant role you have played in the last decade on IT issues. Through your leadership we have all witnessed a substantial increase in attention and efforts to improve the Federal government's management of IT. You have captured the attention of senior policy officials across agencies, challenged Administrations, and as a result have helped to raise focus and understanding of these serious issues, particularly IT security and Y2K.

We all know that our Federal government's IT security problems are serious and pervasive. However, I am pleased to report today that while problems persist, several agencies are demonstrating progress, due in large part to your leadership.

**Government-wide Steps Taken to Improve IT Security**

Since the last hearing in March, a number of achievements have been made toward improving the Federal government's IT security.

1. Provided Congress with Information Requested for Proper Oversight. The combination of the Security Act 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.

2. Developed IT Security Management Performance Measures. OMB issued updated reporting instructions (M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones") to Federal agencies which included objective performance measures. Both agencies and IGs were directed to report the results of their reviews and independent evaluations against those measures. These measures tie directly to the IT security requirements in the Security Act.

3. Developed Government-wide Assessment Tool. The National Institute of Standards and Technology (NIST) developed a security questionnaire in 2001 which greatly assisted agencies in performing self-assessments of their IT systems. This questionnaire was based primarily on NIST technical guidance and the General Accounting Office's Federal Information System Controls Audit Manual and allows agencies to assess the management, operational, and technical controls of their systems. Agencies were directed through OMB guidance to use this document as the basis for conducting their annual reviews under the Security Act. Under NIST's leadership, this questionnaire was automated this year. Agencies now have a free automated tool to assist them in conducting their annual reviews. The tool facilitates IT security reviews while improving the quality of the overall process.

4. Enforcement of Plans of Action and Milestones. This spring, OMB met with agencies (CIO and IG office) to discuss the status of and address deficiencies in their POA&M efforts. Agencies are required to develop POA&Ms for every program and system where an IT security weakness has been found. These plans must be developed, implemented, and managed by the agency official who owns the program or system (program official or Chief Information Officer (CIO) depending on the system) where the weakness was found. 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 has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard.

5. Developed Guidance on Reporting IT Security Costs.

OMB, through Circular A-11 on budget preparation and submission, provided agencies additional guidance in determining IT security costs of their IT investments.

6. Mature IT Security Management Practices. A handful of agencies have demonstrated the maturity of their agency-wide plans of action and milestone (POA&M) process to track and manage remediation of their IT security weaknesses.

7. Government-wide IT Security Training Opportunities.

Through the Administration's electronic government initiative, e-training, IT security courses will be available to all Federal agencies by December. These initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers, and the general workforce.

8. Deployment of E-authentication Capabilities. The E-Authentication e-government initiative deployed 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. Potential agencies that will be using this service include DoEd, USDA/National Finance Center, SSA, and GSA. The full capability is expected in September 2003.

### **Government Information Security Reform - Year Two**

Based primarily on agency and IG reports submitted in September, integration of security into agencies' budget processes, and recently updated and submitted IT security plans of action and milestones, OMB has conducted an initial assessment of the Federal government's IT security status. Due to the baseline of agency IT security performance identified last year, we are now in a position to more accurately determine where progress has been made and where problems remain.

The good news is that for the first time the Federal government's IT security program now has a basic set of IT security performance measures and a comprehensive and uniform process for collecting data against those measures. Additionally:

1. More Departments are exercising greater oversight over their bureaus. This year as part of the reporting instructions, agencies were required to report results at the bureau level;
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;
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; and
5. OMB conditional approval or disapproval of agency IT security programs resulted in senior executives at most agencies paying greater attention to IT security at their agencies.

The bad news is that as we predicted in our previous testimony, the more IT systems that agencies and IG's review, the more security weaknesses they are likely to find. Our initial analysis reveals that while progress has been made, there remain significant weaknesses.

1. 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 assist agencies in prioritizing and reallocating funds to address these problems;
2. Some IGs and CIOs have vastly different views of the state of the agency's security programs. OMB will highlight such discrepancies to agency heads; and
3. 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.

### **Status of Six Common Government-wide IT Security Weaknesses**

In the first annual OMB report to Congress on Federal government information security reform ([www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf](http://www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf)), OMB identified six common government-wide IT security weaknesses along with steps to overcome those weaknesses. I would like to provide you with an update on efforts related to resolving these weaknesses.

1. Lack of agency senior management attention to IT security. In addition to conditionally approving or disapproving agency IT security programs through private communication between OMB and each agency head, OMB used the President's Management Agenda Scorecard to continue to focus agency attention on serious IT security weaknesses. Through the scorecard OMB and senior agency officials monitor agency progress on a quarterly basis.
2. Non-existent IT security performance measures. As I discussed, OMB developed high-level management performance measures to assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific requirements of the Security Act. Agencies were required 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, there are measures for both CIOs and program officials. These measures are mandatory and represent the minimum metrics against which agencies must track to measure performance and progress. We encourage agencies to develop additional measures that address their needs.
3. Poor security education and awareness. As discussed above, for one of the Administration's electronic government initiatives, establishing and delivering electronic-training, IT security training options will be added and available to all Federal agencies in December.
4. Failure to fully fund and integrate 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. As a result, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved 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. Failure to ensure that contractor services are adequately secure. Through the OMB Committee on Executive Branch Information Systems Security, 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. 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. Lack of detecting, reporting, and sharing information on vulnerabilities. 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. It is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center (FedCIRC) and appropriate law enforcement authorities such as the FBI's National Infrastructure Protection Center as required by the Security Act.

GSA recently awarded a contract on patch management. Through this work FedCIRC will be able to disseminate patches to all agencies more effectively. In addition, OMB recently issued guidance to agencies on reporting to FedCIRC, stressing the necessity for accurate and timely reporting while also leveraging an e-business approach that facilitates reporting.

A summary of each agency's security status will be included in the annual OMB report to Congress. We plan on

issuing this report in the same timeframe as the President's budget.

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.

### **Areas for Additional Attention**

OMB, the President's Critical Infrastructure Protection Board, the Federal agencies, and others are also addressing a number of other significant IT security issues.

The Administration strives to ensure that any disruptions to Federal IT systems are infrequent, of minimal duration, manageable, and cause the least damage possible. In that regard, we essentially are addressing two types of threats -- organized (i.e., sophisticated nation states, terrorist, and criminal) and ad hoc (i.e., common hackers of varying levels of sophistication).

Regardless of their level of sophistication (i.e., organized or ad hoc), an attacker can easily exploit numerous vulnerabilities found in today's commercial software products. Some experts estimate that as many as 95% of today's successful attacks exploit these commonly known flaws and most use widely available automated tools to do so. Simple adjustments to out-of-the-box software configurations correct many vulnerabilities and corrective patches are widely available for many others.

We will assure that Federal agencies undertake effective system management practices. This includes tools and training to ensure the timely deployment and continued maintenance of security of IT systems. We are also addressing the out-of-the-box configuration issue. Recently a consortium of Federal agencies and private organizations released security configuration guides for the Windows 2000 operating system. FedCIRC has arranged for download and distribution of the Windows 2000 security testing tool for all Federal civilian agencies.

Countering sophisticated organized threats is far more complex. Many experts consider hostile nation-states and terrorists to pose the greatest threat to the security and

reliability of Federal IT systems. This threat is often associated with the threat of physical attack, and could be used to disrupt government coordination and communication in time of emergency.

The development of a government-wide enterprise architecture is a central part of the Administration's IT management and electronic government efforts. Establishment of an architecture for the Federal government will greatly facilitate more rational IT investment decisions and electronic government. Accordingly, the Administration will be able to better prioritize and fund the Federal government's security needs.

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 developed by the Critical Infrastructure Assurance Office (CIAO) 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, CIAO and OMB will identify cross-government activities and lines of business for Matrix reviews. In this way the Executive Branch will have identified key needs in both vertical and horizontal continuity of operations.

More and more, individual agencies and other organizations have improved means to protect themselves from more sophisticated attackers. Until recently, commercial firewalls and intrusion detection systems primarily defended only against known attacks. New products filter out actions outside normal use, e.g., those activities that are inconsistent with authorized technical "rules" established by systems administrators. Thus even a previously unknown threat can potentially be stopped. We expect that, as it has in the past, the market will continue to produce solutions to security problems.

Among our high-level challenges is identifying the security gaps between agencies with interconnected lines of business. In addition to Project Matrix and the development of the enterprise architecture as a means to address these potential gaps, we will continue to look for other methods as well, through OMB's Committee on Executive Branch Information Systems Security and the CIO Council.

## **Conclusion**

Again Mr. Chairman, I would like to express the Administration's appreciation for your untiring leadership on IT security.

For the first time, through the reporting requirements of the Security Act and agency POA&Ms, we are able to point to real progress in closing the Federal government's IT security performance gaps. While progress has been made both at the government-wide program level as well as within a number of agencies, serious weaknesses, and in some cases repeating weaknesses remain. Failure to meet basic security requirement such as system plans and certifications leaves us with simply unacceptable risks. Our challenge this year is to dramatically build upon this progress to ensure that the Federal government's IT investments are appropriately secured.