

**STATEMENT OF THE HONORABLE KAREN EVANS  
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND  
INFORMATION TECHNOLOGY  
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**

**June 2, 2004**

Good afternoon, Mr. Chairman, Ranking Member Clay, and Members of the Committee. Thank you for inviting me to speak about vulnerability management strategies and technology.

In the past few years, threats in cyberspace have risen dramatically. Many of these threats exploit software flaws which require updates (patches) to correct. Hackers routinely attempt to access networks or disrupt business operations by exploiting software flaws. Because of this threat, Federal CIOs devote considerable resources to the remediation of software vulnerabilities. Systems staff must promptly implement patches as well as other risk reduction measures in order to protect their operating environments from attack while sustaining their current service levels for their customers. This is a difficult challenge. They rely on timely notification of new vulnerabilities and an accurate assessment of the importance of the recommended patch. Due to the large number of vulnerabilities discovered each year (over 3700 in 2003), agencies must correctly determine which patches to implement immediately and which to schedule for the next maintenance cycle. Given the rise in the number of identified vulnerabilities, this task is becoming more and more difficult.

As agencies' information technology security programs mature, the Federal government is moving away from a reactive remediation approach for dealing with IT security vulnerabilities. Through implementation of guidance and policies promoting sound risk management, the use of automated tools, and the emergence of a culture where security is integrated into lifecycle system planning and development; the Federal government is moving towards a more proactive approach to dealing with vulnerabilities within information technology applications, systems, and networks. As a result, we will be able to focus on developing and using security benchmarks, leveraging the government's buying power, and cooperating with industry leaders to promote software development which meets our needs, and is safer "out of the box."

**Strategies to Assess and Reduce Risk**

The Federal government uses several strategies to assess and reduce risks created by software vulnerabilities before they are exploited.

First, CIOs are required by the Paperwork Reduction Act to maintain a current and complete inventory of the agency's information resources. Each system identified in the inventory must undergo a risk assessment and a certification and accreditation (C&A) consistent with Federal standards and guidance. Recent guidance from the National Institute of Standards and Technology (NIST), i.e., Federal Information Processing Standard – 199 “Standards for Security Categorization of Federal Information and Information Systems” and Special Publication 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems,” leads agencies through this careful planning, risk mitigation and testing process before a system is certified to go “on line.” In this way, agencies identify and minimize in advance some of the vulnerabilities posed by malicious code, viruses and worms, and other risks to information or system operations.

In addition to a certifying and accrediting the systems within their inventory, agencies must institute a configuration management process. This process establishes an initial baseline of the configurations associated with hardware and software within the inventory. The configuration management process facilitates changes to the baseline, by ensuring that security configurations are addressed in a standardized manner, to prevent mis-configurations that could permit a vulnerability exploit. Configuration of mobile devices and perimeter security devices such as firewalls and intrusion detection systems are especially important, since these configurations help mitigate risk at the points where an agency's network is vulnerable to external threats. Government laptops should be configured to download the latest anti-virus definitions before they are attached to the network. This helps prevent laptops used outside the agency (e.g., by an employee on travel or working from home) from introducing malicious code when they are brought back into the office for use.

All, IT systems should be securely configured and maintained in accordance with documented security benchmarks. Working with agencies and other industry security experts, organizations such as the Center for Internet Security produces security benchmarks to reduce the likelihood of successful intrusions. Likewise, the National Security Agency (NSA) provides security configuration guides for the Department of Defense and other government agencies. NSA has recently said that they do not intend to publish a separate security guide for Windows Server 2003 beyond what was produced as a cooperative effort between the vendor and the security community. The "High" security settings in Microsoft's "Windows Server 2003 Security Guide" track closely with the security level historically represented in the NSA guidelines. OMB strongly supports these and other industry initiatives to develop best practices for securing products.

The Cyber Security Research and Development Act of 2002 tasks NIST to develop security settings for each hardware or software system that is, or is likely to become, widely used within the Federal Government. Subject to available funds, NIST will maintain a web-based portal and solicit setting recommendations. However, developing

and using security benchmarks is not a trivial task. Obtaining consensus on minimum benchmarks is complex and time consuming.

### **The Pace of the Federal Government's Employment of Strategies to Secure Its Systems**

The Federal Information Security Management Act (FISMA) is a critical mechanism used to drive protection of Federal systems. The Act itself provides a framework for sound IT management. Data collected and reported allows for targeted management and oversight of systems, and allows agencies to assess and make corrections where performance is lacking.

According to our FY03 FISMA data, a number of Departments and agencies had incomplete inventories of hardware and software assets in some cases. Inventories were out of date or did not reflect resources for each of the bureaus. OMB's FY04 FISMA reporting guidance asks Inspectors General (IGs) to comment on whether agencies are updating their inventory at least annually, and whether the agency and the IG agree on the total number of systems.

FISMA requires each agency develop and enforce compliance with specific system configurations. OMB's FY03 reporting guidance sought information on agency progress in meeting this new requirement, but did not judge the adequacy of that process. In OMB's FY04 guidance we are asking agencies to identify the extent to which they are using standard configurations for major operating systems. Both the CIO and the IG must report on the status of agency-wide policies regarding security standard configurations. Additionally, agencies will be asked to list the specific benchmarks which are in use.

Because worms and viruses can cause substantial damage, Federal agencies must take proactive measures to lessen the number of successful attacks. Agencies use anti-virus software with automatic updates in order to detect and block malicious code. DHS' Computer Emergency Readiness Team reports only a few agencies having improperly configured laptops were impacted by the recent Sasser worm. In general, the Federal government has withstood cyber attacks with minimal impact on citizen services.

Patch management is an essential part of an agency's information security program. FY03 FISMA data demonstrates most agencies had formal processes in place for dissemination of patches. However, in several cases, IGs had concerns with the distribution of patches across the enterprise in a timely manner. This year, OMB's FY04 FISMA reporting guidance asks whether agency standard configuration requirements address the patching of security vulnerabilities.

### **Evaluating the Security Profile of Existing Systems**

Under FISMA, Federal agencies are required to periodically test and evaluate the effectiveness of their information security policies, procedures and practices. This

evaluation includes testing the controls of every system identified in the agency's inventory. Last year, the 24 largest agencies reported they had tested an average 64% of their systems. As part of OMB's FY04 FISMA guidance, agencies will be asked to specifically report on their use of vulnerability scans and penetration tests.

Agencies can use a number of commercial products in evaluating compliance with their security policy. For example, the free CIS Scoring Tools provide an easy way for agencies to compare their security configurations against the CIS benchmarks. The scoring tools automatically create reports that direct system administrators to take corrective action when insecure configurations are identified.

### **Use of Automated Tools in Vulnerability Management Strategies**

The Federal government is increasingly using automated tools to monitor the operation of its networks.

Many agencies rely on automated inventory tools to accurately collect hardware and software information from computers across the enterprise. These tools record the presence of unauthorized software as well as outdated software versions. Automated inventory tools reduce the expenditure of staff time and simplify the process of gathering information from computers in multiple locations. Our FY04 FISMA reporting guidance asks agencies to identify tools, techniques and technologies they are using to mitigate internet risk.

In addition, Departments and agencies frequently use system and network vulnerability scanners to quickly identify known weaknesses in their infrastructure. Software scanners locate vulnerabilities using a database of already-catalogued system weaknesses.

One of the most popular resources on NIST's Computer Security Resource Center is the web-based tool known as ICAT. This tool allows users to identify known vulnerabilities and provides links to vendor sites where users can obtain patches. Over 6600 vulnerabilities are now catalogued in this NIST on-line database.

### **Conclusion**

Agencies are continually refining their security management processes to assure vulnerabilities are addressed in a strategic and proactive manner. This is being accomplished through the adherence to guidance and standards, configuration management, the implementation of benchmarking, and the increased use of automated tools to detect and preempt exploits of vulnerabilities. By taking a proactive approach, the Federal Government will be poised to deal with threats that are posed from cyberspace.

OMB will continue to work with agencies and the Congress to ensure that appropriate vulnerability management strategies and technologies are in place. These measures will

minimize disruptions in service and preserve the integrity and availability of Federal IT systems.

Attachment A:

Websites offering security configuration guides:

1. <http://www.cisecurity.org/>
2. <http://nsa2.www.conxion.com>
3. <http://www.microsoft.com/security/guidance/default.aspx>
4. <http://csrc.nist.gov/publications/nistpubs/index.html>

