STATEMENT OF
NORMAN E. LORENTZ
ACTING 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
September 10, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the important topic of worm and virus defense. My testimony today will address how the federal government protects its IT systems from this pervasive threat.

By design, worms and viruses can cause substantial damage and prove disruptive to normal business operations. For this reason, it is important that federal agencies continually and rapidly take proactive measures to lessen the number of successful attacks.

The month of August proved unusually busy for malicious code activity, beginning with the Blaster and then the quickly spreading Sobig.f worm. I am pleased to state that, in general, the federal government withstood these attacks and impact on citizen services was minimal. Agencies have improved their protection against malicious code by installing patches, blocking executables at the firewall, and using anti-virus software with automatic updates.

Agencies did, however, report modest impacts associated with the Blaster and Sobig.f worms. To date, reports from federal civilian agencies show approximately 1000 computers affected by each exploit. This impact ranged from a slowdown in agency e-mail to the temporary unavailability of internal agency systems. A number of laptops proved to be susceptible to infection since configuration management was uneven on these portable devices.

The federal government's ability to thwart worms and viruses depends on a number of interlocking management, technical and operational controls. It is critical that these controls continue to evolve to keep pace with the increasingly sophisticated threat.

<u>How vulnerabilities are discovered</u>

DHS' Federal Computer Incident Response Center (FedCIRC) maintains a strong relationship with a number of industry as well as government partners. These partners include commercial software vendors, Carnegie Mellon University's Computer Emergency Response Team, law enforcement, the intelligence community, and agency incident response teams. These organizations routinely communicate advance notice to DHS regarding the discovery of software vulnerabilities and the development of malicious code designed to exploit these weaknesses.

How Agencies Are Notified About Potential Vulnerabilities

The Federal Computer Incident Response Center within the Department of Homeland Security is the Federal government's focal point for coordinating response to attacks (non-law enforcement), promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. Through this role, FedCIRC notifies Federal agencies about current and potential information security threats and vulnerabilities.

OMB and the CIO Council have developed and deployed a process to rapidly counteract identified threats and vulnerabilities. CIOs are advised via conference call, as well as follow up e-mail, of specific actions needed to protect agency systems. This information is also transmitted to agency incident response centers. Agencies must then report through FedCIRC to OMB on the implementation of the required countermeasures. In particular, we track data concerning the percentage of systems patched and the time needed to complete mitigation efforts. This emergency notification and reporting process was instituted for the Microsoft RPC vulnerability in July and as a result, agencies were able to rapidly close vulnerabilities that otherwise might have been exploited by the Blaster worm.

In analyzing agency responses to earlier OMB data calls, it became apparent that the amount of time needed to implement required fixes was too long and varied widely from agency to agency. OMB asked the CIO Council's Security Liaison to sponsor a meeting so that agencies could share best practices. The meeting ensured that agency CIOs understood the urgency associated with implementing patches and were able to leverage the capabilities and ideas of other agencies.

OMB continued to discuss the Blaster and Sobig.f worms with key agency representatives. Sector specific agencies such as Treasury, Energy and Transportation provided updates on the worm's impact to the private sector and agencies participated in a discussion of lessons learned and next steps. OMB intends to hold after action meetings with federal agencies following all major cyber events so that we may continue to refine this process.

The Mechanisms that Exist for Protecting Systems

The National Institute of Standards and Technology (NIST) provides guidelines to federal agencies on securing networks, systems, and applications. NIST recommends that agencies implement a patch management program, harden all hosts appropriately, deploy antivirus software to detect and block malicious code, and configure the network perimeter to deny all traffic that is not necessary. Additional recommendations include user awareness briefings as well as training for technical staff on security standards, procedures, and sound security practices. Per longstanding OMB policy, Federal agencies are directed to follow NIST guidelines.

NIST has produced a number of recent publications that address agency security practices. These publications include: Securing the Public Web Server, Electronic Mail Security, IT Contingency Planning, Security Metrics, System Administrator Guidance for Securing Win

2000, Wireless Security, Security Patch Management, Intrusion Detection Systems, Firewall Security, and Risk Management.

As part of its statutory responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology will publish in September draft guidelines for incident handling. The guidelines will discuss how to establish and maintain an effective incident response program with an emphasis on incident detection, analysis, prioritization and containment. The guidelines will include recommendations for handling certain types of incidents, such as distributed denial of service attacks and malicious code infections. In addition, the guidelines will include a set of sample incident scenarios that can be used to perform incident response team exercises. The guidelines will be written so they can be followed regardless of hardware platform, operating system, protocol, or application.

Another critical mechanism used to enforce protection of Federal systems is the Federal Information Security Management Act (FISMA). Under FISMA, Federal agencies are required to periodically test and evaluate the effectiveness of their information security policies, procedures and practices. The results of both the agency self assessments and the IG assessments are provided to OMB each September. OMB submits a summary report to Congress based on the agency and IG reports.

The Problems Presented by Patching Systems

Patch management is an essential part of an agency's information security program and requires a substantial investment of time and effort. Agencies must carefully follow predefined processes in order to successfully remediate system vulnerabilities across the enterprise.

These processes include: identifying all affected systems and related software revision levels, fully testing the patch before it is placed into a production environment, and prioritizing installation of the patch based on the criticality of the system. Alternative solutions such as judicious use of port blocking must be implemented if the patch cannot be installed.

A number of agencies utilize automated tools to push patches to the desktop. The automation of the patch management process is significantly easier if the agency maintains standardized software configurations.

At the present time, forty-seven agencies subscribe to FedCIRC's Patch Authentication and Dissemination Capability. This service validates and quickly distributes corrective patches for known vulnerabilities.

Federal Enterprise Architecture

Improving the federal government's response to malicious code requires that we focus on enterprise architecture and the standardized deployment of security technologies. As new technologies become available and cost effective, they must be incorporated into the IT infrastructure where they can monitor common precursors and indications of attack.

Conclusion

The Federal government is the world's largest consumer of IT systems. Because of its vast inventory and the vulnerabilities inherent in commercial software, the Federal government will, for the immediate future, continue to be impacted by the proliferation of worms and viruses. Through our oversight of agency security policies and practices, OMB will continue to work with agencies to ensure that the risks associated with malicious code are appropriately mitigated.

In addition, the federal government will continue to rely on federal, state and local law enforcement to investigate and prosecute developers of malicious code. Agencies must continue to report computer incidents and assist law enforcement investigations to the greatest extent possible. Strong cooperation was displayed between the FedCIRC community and the Secret Service, FBI and other law enforcement officials during the recent Blaster and Sobig.F incidents.

In closing, OMB is committed to a federal government with resilient information systems. Worms and viruses must not be allowed to significantly affect agency business processes. OMB will continue to work with agencies and the Congress to ensure that appropriate countermeasures are in place to reduce the impact of malicious code.