

TOM DAVIS, VIRGINIA,  
CHAIRMAN

DAN BURTON, INDIANA  
CHRISTOPHER SHAYS, CONNECTICUT  
ILEANA ROS-LEHTINEN, FLORIDA  
JOHN M. McHUGH, NEW YORK  
JOHN L. MICA, FLORIDA  
MARK E. SOUDER, INDIANA  
STEVEN C. LATOURETTE, OHIO  
DOUG OSE, CALIFORNIA  
RON LEWIS, KENTUCKY  
JO ANN DAVIS, VIRGINIA  
TODD RUSSELL PLATTS, PENNSYLVANIA  
CHRIS CANNON, UTAH  
ADAM H. PUTNAM, FLORIDA  
EDWARD L. SCHROCK, VIRGINIA  
JOHN J. DUNCAN, JR., TENNESSEE  
NATHAN DEAL, GEORGIA  
CANDICE MILLER, MICHIGAN  
TIM MURPHY, PENNSYLVANIA  
MICHAEL R. TURNER, OHIO  
JOHN R. CARTER, TEXAS  
MARSHA BLACKBURN, TENNESSEE  
PATRICK J. TIBERI, OHIO  
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS

# Congress of the United States

## House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
FACSIMILE (202) 225-3974  
MINORITY (202) 225-5051  
TTY (202) 225-6852

[www.house.gov/reform](http://www.house.gov/reform)

HENRY A. WAXMAN, CALIFORNIA,  
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA  
MAJOR R. OWENS, NEW YORK  
EDOLPHUS TOWNS, NEW YORK  
PAUL E. KANJORSKI, PENNSYLVANIA  
CAROLYN B. MALONEY, NEW YORK  
ELIJAH E. CUMMINGS, MARYLAND  
DENNIS J. KUCINICH, OHIO  
DANNY K. DAVIS, ILLINOIS  
JOHN F. TIERNEY, MASSACHUSETTS  
WM. LACY CLAY, MISSOURI  
DIANE E. WATSON, CALIFORNIA  
STEPHEN F. LYNCH, MASSACHUSETTS  
CHRIS VAN HOLLEN, MARYLAND  
LINDA T. SANCHEZ, CALIFORNIA  
C.A. DUTCH RUPPERSBERGER,  
MARYLAND  
ELEANOR HOLMES NORTON,  
DISTRICT OF COLUMBIA  
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT,  
INDEPENDENT

### SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Congressman Adam Putnam, Chairman



#### OVERSIGHT HEARING STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: *“Who Might be Lurking at Your Cyber Front Door?  
Is Your System Really Secure?  
Strategies and Technologies to Prevent, Detect and Respond to the Growing Threat of  
Network Vulnerabilities.”*

Wednesday, June 2, 2004  
1:30 p.m.  
Room 2154, Rayburn House Office Building

#### OPENING STATEMENT

Good afternoon and welcome to the Subcommittee’s hearing entitled - “Who Might be Lurking at Your Cyber Front Door? Is Your System Really Secure?” Today we continue our in-depth review of cyber security issues affecting our Nation.

The Internet has created a global network of systems that have improved the quality of our lives, created unprecedented communication capabilities, and increased our productivity. The interdependent nature of these systems has also unleashed the potential for world-wide cyber attacks that can infect hundreds of thousands of computers in just hours.

Since 1999, the number of cyber attacks has grown and is continuing to grow at an alarming rate. The cost of preventing and responding to these attacks is staggering; some estimate that the economic impact from digital attacks in 2004 will be in the billions. While opinions may differ on the cost of the impact, there is clear evidence that the effect on the private and public sectors is significant.

Preventing cyber attacks and the damages caused by them pose some very unique and menacing challenges. Our critical infrastructure and government systems can be – and are being – attacked from anywhere ... at any time. Cyber criminals, disgruntled insiders, hackers, enemy states, and those who wish us harm are constantly seeking to steal confidential information as well as hijack vulnerable computers, and then turn them into zombies that can be used to carry out malicious activities. This is a global ... 24 hours a day, 7 days a week ... challenge. There can be no down time when it comes to protecting our Nation's critical infrastructure.

Of even greater concern, we know that various terrorist groups possess advanced vulnerability scanning capabilities and are very sophisticated – and becoming increasingly more so each and every day. The combination of a cyber attack in conjunction with a physical attack could magnify the effects of the physical destruction and create even greater mayhem. We all have a role and responsibility in taking appropriate measures to reduce the risk and improve our overall information security profile.

As a Nation, we have taken very dramatic steps to increase our physical security, but protecting our information networks has not progressed at the same pace ... either in the public ... or in the private sector. The Department of Homeland Security is working to make strides in this area. Although I acknowledge the efforts of the National Cyber Security Division, I am still concerned that we are *collectively* not moving fast enough to protect the American people and the U. S. economy from the very real threats that exist today. Make no mistake. The threat is serious. The vulnerabilities are extensive. And the time for action is NOW!

New vulnerabilities in software and hardware products are discovered constantly. According to the CERT Coordination Center, as of the end of 2003 there are over 12,000 known vulnerabilities that could be exploited. These vulnerabilities span across thousands of products from many different vendors. With the increasing complexity and size of software programs, we will probably never reach a point where no new vulnerabilities are discovered. However, we need to continue to strive to improve and to develop more advanced tools for testing and evaluating code.

The problem of newly discovered vulnerabilities is compounded by the fact that the window that the good guys have is closing; attackers are exploiting published vulnerabilities faster than ever. The recent Sasser worm outbreak occurred just seventeen days after the patch was released; although it was largely contained, it still caused significant disruptions around the globe.

In addition to the shrinking period from patch to exploit, attackers are finding faster ways to exploit existing vulnerabilities previously deemed low risk. For example, in April of this year, a researcher reported he was able to exploit quickly a previously known flaw in some of the underlying Internet traffic technology. It was thought to take between 4 and

142 years to exploit this flaw. The researcher cut the exploit time down to just a matter of seconds

The rise of mobile computing further complicates the vulnerability issue. Laptops that were not connected to a network when the latest patches were released can pick up a worm or virus and become time bombs waiting to go off when reconnected to the network. Remote access presents its own set of new and growing vulnerability challenges.

Not only is the sheer quantity of patches and systems overwhelming for administrators to keep up with, but also patches can have unexpected side effects on other system components resulting in losses of system availability. As a result, after a patch is released, system administrators often take a long time to fix all their vulnerable computer systems. Configuration management is a key element of vulnerability management, and it is more challenging in the federal government, which has many legacy systems running customized applications that can be very difficult to patch when a new vulnerability arises.

Clearly the challenge of vulnerability management is great. We must ensure that current systems are cleaned and protected while at the same time ensuring that new systems do not become victims. There are tools and strategies available to help achieve these goals. According to at least one estimate, about 95 percent of all network intrusions could be avoided by keeping systems secure through the effective use of vulnerability management strategies.

We need to focus our vulnerability management efforts on three key ingredients: prevention; detection; and response.

Prevention—we need to do our best to reduce the impact of inevitable software and hardware vulnerabilities. That means having systems appropriately identified, configured and patched. That means producing more secure software and hardware. That means using new technologies, processes and protocols to stop attacks dead in their tracks before an intrusion occurs.

Detection—Even with a strong program of protection, network intrusions are likely to continue. Detection requires laser like focus. We must always be on our guard so that no intrusion goes unnoticed. This means a program that includes vulnerability scanning and intrusion detection capabilities.

Response—once we have detected an attack, we need to have ways to isolate the intrusion attempt, trigger an incident response plan when appropriate and limit the potential impact on the system.

Vulnerability management is especially important in federal systems. This Subcommittee has aggressively overseen implementation and compliance with the requirements of the Federal Information Security Management Act (FISMA). FISMA provides a comprehensive risk management framework for information security in federal departments and agencies. At the end of last year, this Subcommittee released the 2003 report card detailing the largest federal departments and agencies progress in implementing FISMA. Overall, for 2003, the federal government received a grade of “D”, a slight improvement over the “F” the government received in 2002.

The reports behind the grades revealed troubling signs of weakness within the federal government's information security. Out of the 24 largest departments and agencies, only five agencies had completed reliable inventories of their critical IT assets leaving 19 without reliable inventories. This is very troubling considering we are four years into this process and still we have far too many agencies with incomplete inventories. How can you secure what you don't know you have? How can you claim to have completed a certification and accreditation process absent a reliable inventory of your assets?

Cyber attackers specifically target the federal government because of the high value of penetrating or taking over government systems. A myriad of automated attack tools are operating around the clock scanning the Internet for systems that can be taken over. Certain experts suggest that some federal systems have already been compromised and are being used as attack tools even as I speak. I am greatly concerned not only how future systems will be protected but also how the federal government will take the necessary steps to prove the security and integrity of its current systems. These security gaps will persist until federal agencies are able to appropriately track the vulnerability status of all of their systems using accurate and complete agency inventories.

For the future, I will continue to monitor the agencies' implementation of FISMA and OMB's guidance to agencies on implementing FISMA. Specifically, I would like to see more detailed guidance and enforcement of FISMA's configuration management provisions. Also, with the termination of the federal patch service, known as PADC, in February 2004, I am looking to OMB as well as the Department of Homeland Security for their thoughts about the feasibility of providing centralized patch management services to civilian agencies as part of an overall vulnerability management strategy.

In conjunction with my oversight of federal information security, I remain deeply concerned about the state of information security in the private sector. 85% of this nation's critical infrastructure is owned or controlled by the private sector, thus maintaining its integrity and availability is critical to the continued success of the Nation's economy and protection of the American people.

Worms, viruses, hacking, identity theft, fraud, extortion and industrial espionage continue to rise exponentially in frequency, severity and financial cost. Last year alone, cyber attacks cost the U.S. financial sector nearly \$1 billion, according to BITS, a nonprofit financial services industry consortium.

Business leaders are responsible for doing their part to improve the security of their information systems. I have called on businesses of all sizes throughout America to consider the matter of information security as it relates to their business. Some businesses are clearly elements of the nation's critical infrastructure and require a more robust risk management plan; however, every business has a responsibility to practice at least basic information security hygiene and to do their part to contribute to the overall security of computers and information networks in this country.

Vulnerabilities in software, and the worms and viruses that exploit them, have become a fact of life for the Internet. The government, law enforcement, researchers, and private industry must join together to protect the vital structure of the Internet, and cyber criminals must be rooted out and brought to justice. Progress is being made, but security is a journey that never ends.

Today's hearing is an opportunity to examine: the challenges in managing information system vulnerabilities; strategies to assess and reduce the risks created by these vulnerabilities; the pace of the federal government's and the private sector's employment of these strategies in securing their own systems; and how automated tools should be employed in applying these strategies.

I eagerly look forward to the expert testimony that our distinguished panel of leaders in information security will provide today as well as the opportunity to discuss the challenges that lie ahead.

#####