AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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

HEARING

BEFORE THE

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

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 2, 2004

Serial No. 108–232

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

96–992 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

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 S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
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)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

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

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
DAN DALY, *Professional Staff Member*
JULIANA FRENCH, *Clerk*
ADAM BORDES, *Minority Professional Staff Member*

CONTENTS

Page

Hearing held on June 2, 2004 1

Statement of:

Beinhorn, Dubhe, vice president, Juniper Federal Systems; Scott Culp, senior security strategist, Microsoft Corp.; Louis Rosenthal, executive vice president, ABN Amro Services Co., Inc.; Marc Maiffret, chief hacking officer, eEye Digital Security; and Steve Solomon, chief executive officer, Citadel Security Software, Inc. 92

Evans, Karen, Administrator, E-Government and Information Technology, Office of Management and Budget; Robert Dacey, Director, Information Security Issues, U.S. General Accounting Office; Amit Yoran, Director, National Cyber Security Division, Department of Homeland Security; Dawn Meyerriecks, Chief Technology Officer, Defense Information Systems Agency, Department of Defense; and Daniel Mehan, Assistant Administrator, Information Services and Chief Information Officer, Federal Aviation Administration 11

Letters, statements, etc., submitted for the record by:

Beinhorn, Dubhe, vice president, Juniper Federal Systems, prepared statement of 95

Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of 79

Culp, Scott, senior security strategist, Microsoft Corp., prepared statement of 102

Dacey, Robert, Director, Information Security Issues, U.S. General Accounting Office, prepared statement of 21

Evans, Karen, Administrator, E-Government and Information Technology, Office of Management and Budget, prepared statement of 14

Maiffret, Marc, chief hacking officer, eEye Digital Security, prepared statement of 134

Mehan, Daniel, Assistant Administrator, Information Services and Chief Information Officer, Federal Aviation Administration, prepared statement of 70

Meyerriecks, Dawn, Chief Technology Officer, Defense Information Systems Agency, Department of Defense, prepared statement of 56

Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of 6

Rosenthal, Louis, executive vice president, ABN Amro Services Co., Inc., prepared statement of 125

Solomon, Steve, chief executive officer, Citadel Security Software, Inc., prepared statement of 153

Yoran, Amit, Director, National Cyber Security Division, Department of Homeland Security, prepared statement of 44

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

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:40 p.m., in room 2154, Rayburn House Office Building, Hon. Adam H. Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Dan Daly, professional staff member and deputy counsel; Juliana French, clerk; Felipe Colon, fellow; Kaitlyn Jahrling and Collin Samples, interns; Adam Bordes and David McMillen, minority professional staff members; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good afternoon. Welcome back. I hope everyone had a nice Memorial Day respite from dealing with Congress.

Today's subcommittee hearing is entitled, "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" 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 communications capabilities and increased productivity. The interdependent nature of these systems has also unleashed the potential for worldwide cyber attacks that can affect hundreds of thousands of computers in mere hours. Since 1999, the number of cyber attacks has grown and continues 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 im-

pact, there is clear evidence that the effect on private and public sectors is significant.

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

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

In preparation for this hearing, the subcommittee traveled to the NSA yesterday and continued to be impressed with the work that is going on out there. We appreciate the efforts of that agency.

As a Nation, we have taken 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. I acknowledge the efforts of the National Cyber Security Division but I remain concerned that we are collectively not moving fast enough to protect the American people and the U.S. economy from the 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 at the end of 2003, there were over 12,000 known vulnerabilities that could be exploited. They span across thousands of products from a number of different vendors. With the increasing complexity and size of software programs, we likely will never reach a point where no new vulnerabilities are discovered. However, we need to continue to strive to improve and develop more advanced tools for testing and evaluating code.

The problem of newly discovered vulnerabilities is compounded by the fact that the window the good guys have is closing. Attackers are exploiting published vulnerabilities faster than ever. The recent Sasser worm outbreak occurred just 17 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. 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 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 other vulnerable computer systems. Configuration management is a key element of vulnerability management and it is more challenging in the Federal Government, which has a number of legacy systems running customized applications that can be 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, 95 percent of all network intrusions could be avoided by keeping systems secure through effective use of vulnerability management strategies. We need to focus our vulnerability management efforts on three key ingredients: prevention, detection and response.

For 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. It means producing more secure software and hardware. It means using new technologies, processes and protocols to stop attacks dead in their tracks before intrusion occurs.

Detection, even with a strong program of protection, network intrusions are likely to continue. Detection requires laser 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. Vulnerability management is especially important in Federal systems. This subcommittee has aggressively overseen implementation and compliance with requirements of FISMA. FISMA provides a comprehensive risk management framework for information security in Federal departments and agencies. At the end of last year, we released a report card detailing the largest Federal departments and agencies progress in implementing FISMA. In 2003, the overall Federal Government received a grade of "D," a slight improvement over the grade of "F" it received in 2002. The reports behind the grade reveals troubling signs of weakness within the Federal Government's information security. Of the 24 largest departments and agencies, only 5 had completed inventories of their critical IT assets, leaving 19 without. This is troubling considering we are 4 years into this process and still have far too many agencies with incomplete inventories.

As we have said in the past, you can't secure what you don't know you have. You can't claim to have completed the certification and accreditation process without a reliable inventory of 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 to be taken over. Experts suggest that some Federal systems have already been compromised and are being used as attack tools even as we speak. I am concerned not only how future systems will be protected but also how the Federal Government will take the necessary steps to improve the security and integrity of current systems. These gaps will persist until Federal agencies are able to appropriately track the vulnerability status of all of their systems using accurate and complete inventories.

For the future, we 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 [FPS], 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 oversight of Federal information security, I remain deeply concerned about the state of information security in the private sector. Eighty-five percent of the 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, identify theft, fraud, extortion and industrial espionage continue to rise exponentially in frequency, severity and cost. Last year alone, cyber attacks cost the U.S. financial sector nearly $1 billion according to BITS, a non-profit financial service industry consortium. Business leaders are responsible for doing their part to improve the security of information systems. I have called on businesses of all sizes throughout the country 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 do their part to contribute to the overall security of computers and networks in this Nation.

Vulnerabilities in software and 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. Some 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 risk created by these vulnerabilities, the pace of the

Government and private sector's employment of these strategies in securing their own systems and how automated tools should be employed in applying those strategies.

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

[The prepared statement of Hon. Adam H. Putnam follows:]

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

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.

#####

Mr. PUTNAM. We will await the distinguished ranking member's testimony and insert it in the record at the appropriate time. With that, we will go ahead and ask the first panel and anyone accompanying you to provide corollary information to the subcommittee to please rise for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. I would note for the record all the witnesses responded in the affirmative. We will begin the testimony of panel I with Ms. Evans. On September 3, 2003, Karen Evans was appointed by President Bush to be Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. Prior to joining OMB, Ms. Evans was Chief Information Officer of the Department of Energy and served as vice chairman of the CIO Council. Before that, she served at the Department of Justice as Assistant and Division Director for Information Systems Management.

Welcome to the subcommittee. You are recognized.

STATEMENTS OF KAREN EVANS, ADMINISTRATOR, E-GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; ROBERT DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE; AMIT YORAN, DIRECTOR, NATIONAL CYBER SECURITY DIVISION, DEPARTMENT OF HOMELAND SECURITY; DAWN MEYERRIECKS, CHIEF TECHNOLOGY OFFICER, DEFENSE INFORMATION SYSTEMS AGENCY, DEPARTMENT OF DEFENSE; AND DANIEL MEHAN, ASSISTANT ADMINISTRATOR, INFORMATION SERVICES AND CHIEF INFORMATION OFFICER, FEDERAL AVIATION ADMINISTRATION

Ms. EVANS. Good afternoon, Mr. Chairman. Thank you for inviting me to speak about vulnerability management strategies and technologies.

In the past few years, threats in cyber space have risen dramatically. Hackers routinely attempt to access networks and to disrupt business operations by exploiting software flaws. Because of this threat, Federal CIOs devote considerable resources to the remediation of software vulnerabilities. Currently, due to the large number of vulnerabilities discovered each year, agencies must correctly determine which patches to implement immediately and which to schedule for the next maintenance cycle, while sustaining their current service levels for their customers. Given the rise in the number of identified vulnerabilities, this task is becoming more and more of a challenge. 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 that promote sound risk management, the use of automated tools and development of a culture where security is ingrained in planning and development of systems life cycles, the Federal Government is evolving toward a more proactive approach to deal with vulnerabilities existing within information technology applications systems and networks. As a result, we will be able to focus resources on analytical trend analysis, the use of benchmarks, leveraging buying power and cooperative work with industry lead-

ers to ensure software development meets our needs and is safer out of the box.

The Federal Government uses several preemptive strategies to assess and reduce the risk created by software vulnerabilities before vulnerabilities are exploited. First, CIOs are required by the Paperwork Reduction Act to maintain a current and complete inventory of the agencies' information resources. Each system identified in the inventory must undergo a threat assessment and a certification and accreditation [C&A] consistent with national standards and guidance.

In addition to a system inventory and required system C&A's, agencies must institute a configuration management process. This process is intended to be closely tied to the system inventory, establishing an initial baseline of the configurations associated with existing hardware and software. The purpose of a configuration management process is to facilitate change to the baseline by ensuring security configurations are addressed in a standardized manner. This helps to prevent misconfigurations leading to vulnerability exploits. Configuration of mobile devices and perimeter security devices such as firewalls and intrusion detection systems are especially important since configurations help to mitigate risk at points where the agency's network is vulnerable to threats from outside their own network.

All IT systems should be configured in accordance with security benchmarks. Working with the agencies and other industry security experts, organizations such as the Center for Internet Security produce security benchmarks to reduce the likelihood of successful intrusions. Likewise, NSA provides security configuration guides to the Department of Defense and other Government agencies. The Cyber Security Research and Development Act formally tasks the National Institute of Standards and Technology to develop security settings for each hardware and software system that is or is likely to be used within the Federal Government. The Federal Information Security Management Act [FISMA], is a critical mechanism used to drive protection of Federal systems. According to fiscal year 2003 FISMA data, a number of departments and agencies in some cases had incomplete inventories of hardware and software assets. OMB's fiscal year 2004 FISMA reporting guidance asks the agency's inspector generals 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 to develop and enforce compliance with specific system configurations. This year both the CIO and the IG must report on the status of agency-wide policies regarding standard security 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 antivirus software with automatic updates in order to detect and block malicious code. DHS' Computer Emergency Readiness Team reports only a few agencies were impacted by the recent Sasser worm. In general, the Federal Government has withstood cyber attacks with minimum impact on citizens. Patch management is an essential part of the agency's information

security program and although fiscal year 2003 FISMA data demonstrates that most agencies had a formal process in place for the dissemination of security patches, in several cases IGs had concerns with the timeliness of the distribution of patches. OMB's fiscal year 2004 FISMA reporting guidance asks whether agency configuration requirements address the patching of security vulnerabilities.

Federal agencies are required to test the technical controls of every system identified in the agency's inventory. Last year, the 24 largest agencies reported that they had tested an average of 64 percent of their systems. As part of OMB's fiscal year 2004 FISMA guidance, agencies will be asked to specifically report on the use of vulnerability scans and penetration testing. 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. Departments and agencies frequently use system and network vulnerability scanners to quickly identify known weaknesses in their infrastructures. Software scanners locate the vulnerabilities using the data base of already catalogued system weaknesses.

Agencies are constantly refining their management processes to assure risks and threats from vulnerabilities are being handled in a strategic and proactive manner. This is being accomplished through the adherence to guidance and standards, configuration management, 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 posed from cyber space. OMB will continue to work with the agencies and the Congress to ensure appropriate vulnerability management strategies and technologies are in place. These measures will minimize disruption and service and preserve the integrity and the availability of Federal systems.

I am pleased to take questions at this time.

[The prepared statement of Ms. Evans follows:]

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.

Mr. PUTNAM. Thank you, Ms. Evans.

Our next witness is Robert Dacey. Mr. Dacey is currently Director of Information Security Issues, U.S. General Accounting Office. His responsibilities include evaluating information system security in Federal agencies and corporations, assessing the Federal infrastructure for managing information security, evaluating the Federal Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats and identifying best security practices of leading organizations and promoting their adoption by Federal agencies.

In addition to many years of information security auditing, Mr. Dacey has also previously led several GAO financial audits.

You are recognized for 5 minutes. Welcome to the subcommittee.

Mr. DACEY. Mr. Chairman, members of the subcommittee, I am pleased to be here today to discuss patch management and steps agencies can take to mitigate information security risks resulting from software vulnerabilities. Today we are releasing our more detailed report on this subject which was requested by this subcommittee as well as the full committee. As you requested, I will briefly summarize my written statement.

The exploitation of software vulnerabilities by hackers and others can result in significant damage to both Federal and non-Federal operations and assets ranging from Web site to defacement to gaining the ability to read, modify or delete sensitive information, destroy systems, disrupt operations or launch attacks against other organizations. Such risks continue to grow with the increasing volume of reported security vulnerabilities, the increasing complexity and size of computer programs, the increasing sophistication and availability of easy to use hacking tools, the decreasing length of time from the announcement of a vulnerability until it is exploited, which is evidenced by the chart on the easel. As you can see, that has been steadily decreasing to the point where we will have exploits within a day of the announcement of vulnerability, so-called zero day exploits and those are becoming more commonplace as we go forward. Another risk factor is the decreasing length of time for attacks to propagate throughout the Internet.

There have been a number of Federal efforts to address patch management which Ms. Evans summarized, including the FISMA reporting requirements as well as guidance. Also, a number of commercial tools and services are available to assist agencies in performing patch management functions more efficiently and effectively.

In our testimony last September before this subcommittee, we described several key elements of an effective patch management program, including standardizing policies, procedures and tools, performing risk assessments and testing patches, and monitoring system status. Responses to our survey of 24 major Federal agencies included the reported status of agency information and implementation of these key patch management practices.

All 24 agencies consistently reported having adopted certain of these practices, including involving senior management, developing system inventories, and providing information security training. However, agency implementation of other key practices varied. For example, one-third reported not having developed agencywide

patch management policies and about 40 percent reported having no agencywide patch management procedures in place.

Two, just under half of the 24 agencies said they performed documented risk assessments of all major systems to determine whether to apply a patch or work around, while others reported they considered various factors before implementing the patch. While all 24 agencies reported that they test some patches before deployment, only about 40 percent reported testing all and only 4 of the 24 reported they monitor all of their systems on a regular basis to assess their networks and patch status, while others indicated they performed some level of monitoring activities. Without consistent implementation of patch management practices, agencies are at increased risk of attacks that can exploit software vulnerabilities in their systems.

Security experts and agency officials identified several challenges to implementing effective patch management practices, including the high volume and frequency of patches, the patching of heterogeneous systems typically found in Federal agencies, ensuring mobile systems receive the latest patches, patching high availability systems and dedicating sufficient resources to patch management. In our report with which OMB generally agreed, we recommend that OMB instruct agencies to provide more refined information on patch management practices in their FISMA reports and to determine the feasibility of providing selected centralized patch management services to assist Federal agencies.

In addition to implementing effective patch management practices, our report also identifies several additional steps that can be taken to address software vulnerabilities including, one, employing more rigorous software engineering practices to reduce the number of potential vulnerabilities; two, deploying a layered defense in-depth strategy against attacks; three, ensuring strong configuration management and contingency planning practices; and four, researching and developing new technologies to better prevent, detect and recover from attacks as well as to identify perpetrators.

Mr. Chairman and members of the subcommittee, this concludes my statement. I would be pleased to answer any questions you or other members of the subcommittee may have at this time.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 1:30 p.m. EDT
Wednesday, June 2, 2004

INFORMATION SECURITY

Agencies Face Challenges in Implementing Effective Software Patch Management Processes

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-04-816T

June 2, 2004

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-04-816T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

INFORMATION SECURITY

Agencies Face Challenges in Implementing Effective Software Patch Management Processes

Why GAO Did This Study

Flaws in software code can introduce vulnerabilities that may be exploited to cause significant damage to federal information systems. Such risks continue to grow with the increasing speed, sophistication, and volume of reported attacks, as well as the decreasing period of the time from vulnerability announcement to attempted exploits. The process of applying software patches to fix flaws–patch management–is critical to helping secure systems from attacks.

At the request of the Committee on Government Reform and this Subcommittee, GAO reviewed the (1) reported status of 24 selected agencies in performing effective patch management practices, (2) tools and services available to federal agencies, (3) challenges to this endeavor, and (4) additional steps that can be taken to mitigate risks created by software vulnerabilities. This testimony highlights the findings of GAO's report, which is being released at this hearing.

What GAO Recommends

In its report, GAO recommends that the Office of Management and Budget (OMB) instruct agencies to provide more refined information on their patch management practices in their annual reports and determine the feasibility of providing selected centralized services to federal civilian agencies. OMB concurs with these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-816T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

Agencies are generally implementing certain common patch management-related practices, such as inventorying their systems and providing information security training. However, they are not consistently implementing other common practices. Specifically, not all agencies have established patch management policies and procedures. Moreover, not all agencies are testing all patches before deployment, performing documented risk assessments of major systems to determine whether to apply patches, or monitoring the status of patches once they are deployed to ensure that they are properly installed.

Commercial tools and services are available to assist agencies in performing patch management activities. These tools and services can make patch management processes more efficient by automating time-consuming tasks, such as scanning networks and keeping up-to-date on the continuous releases of new patches.

Nevertheless, agencies face significant challenges to implementing effective patch management. These include, among others,

- the high volume and increasing frequency of needed patches,
- patching heterogeneous systems,
- ensuring that mobile systems such as laptops receive the latest patches, and
- dedicating sufficient resources to assessing vulnerabilities and deploying patches.

Agency officials and computer security experts have identified several additional measures that vendors, the security community, and the federal government can take to address the risks associated with software vulnerabilities. These include, among others, adopting more rigorous software engineering practices to reduce the number of coding errors that create the need for patches, implementing successive layers of defense mechanisms at strategic points in agency information systems, and researching and developing new technologies to help uncover flaws during software development.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss patch management[1] and steps that agencies can take to mitigate information security risks resulting from software vulnerabilities. As you know, attackers may attempt to exploit such vulnerabilities, potentially causing significant damage to agencies' computer systems.

My testimony today will highlight the findings of a report requested by the Subcommittee and full Committee, which we are releasing today.[2] This report discusses: (1) the status of 23 of the agencies under the Chief Financial Officers (CFO) Act of 1990[3] and the Department of Homeland Security (DHS) in performing effective patch management, (2) tools and services available to assist federal agencies in this endeavor, (3) obstacles to performing effective patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities.

Our report is based on an extensive search of professional information technology (IT) security literature, research studies and reports about cybersecurity-related vulnerabilities (including our own), and the results of a Web-based survey of the 24 agencies that we conducted to determine their patch management practices. Our work was conducted from September 2003 through last month, in accordance with generally accepted government auditing standards.

Results in Brief

As our report discusses in detail, agencies are generally implementing certain important patch management-related

[1]Patch management is the process of applying software patches to correct flaws. A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

[2]U.S. General Accounting Office, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

[3]31 USC Section 901.

practices, such as inventorying their systems and providing information security training. However, they are not consistently performing other critical practices, such as testing all patches before deployment to help determine whether the patch functions as intended and to ascertain its potential for adversely affecting an agency's system.

Several automated tools and services are available to assist agencies in performing patch management. These typically include a wide range of functionality, including methods to inventory computers, identify relevant patches and workarounds, test patches, and report network status information to various levels of management.

Agencies face several obstacles in implementing effective patch management practices, including (1) installing patches quickly while at the same time testing them adequately before installation, (2) patching heterogeneous systems, (3) ensuring that mobile systems receive the latest patches, (4) avoiding unacceptable downtime when patching systems that require a high degree of availability, and (5) dedicating sufficient resources to patch management.

Agency officials and computer security experts identified several additional steps that could be taken by vendors, the security community, and the federal government to assist agencies in overcoming such challenges. For example, more rigorous software engineering by vendors could reduce the number of vulnerabilities and the need for patches. In addition, the federal government could use its substantial purchasing power to influence software vendors to deliver more security systems.

Our report recommends that the Director, Office of Management and Budget (OMB), (1) instruct agencies to provide more refined information on their patch management practices in their annual Federal Information Security Management Act (FISMA) of 2002[4] reports, and (2) determine the feasibility of providing selected centralized patch management services to federal civilian agencies, incorporating lessons learned from a now-discontinued service

[4]Pub. L. 107-347, Title III, December 17, 2002.

initiated by the Federal Computer Incident Response Center (FedCIRC). OMB generally agrees with our findings and recommendations.

Background

Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management,[5] it includes acquiring, testing, applying, and monitoring patches to a computer system. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows 2000 reportedly contains about 35 million lines of code, compared with about 15 million lines for Windows 95. As reported by the National Institute of Standards and Technology (NIST), based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.[6]

Security Vulnerabilities and Incidents Are Increasing

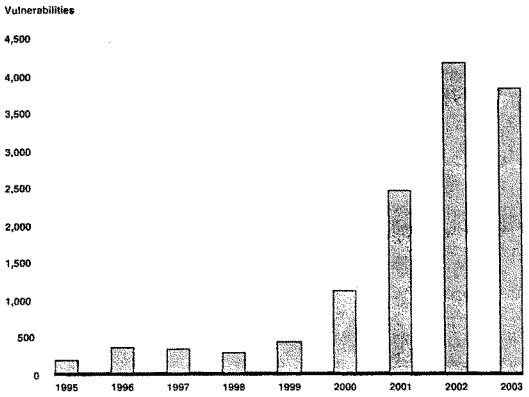
From 1995 through 2003, the CERT® Coordination Center (CERT/CC)[7] reported just under 13,000 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities during this period.

[5]Configuration management is the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of a system.

[6]National Institute of Standards and Technology, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (Gaithersburg, Md.: August 2002).

[7]CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie-Mellon University.

Figure 1: Security Vulnerabilities, 1995–2003



Source: GAO analysis based on Carnegie Mellon University's CERT® Coordination Center data.

As vulnerabilities are discovered, attackers can cause major damage in attempting to exploit them. This damage can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; destroy systems; disrupt operations; or launch attacks against other organizations' systems. Attacks can be launched against specific targets or widely distributed through viruses and worms.[8]

The sophistication and effectiveness of cyber attacks have steadily advanced. According to security researchers, reverse-engineering patches has become a leading method for exploiting vulnerabilities.

[8]A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. In contrast, a worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

By using the same tools used by programmers to analyze malicious code and perform vulnerability research, hackers can locate the vulnerable code in unpatched software and build to exploit it. Reverse engineering starts by locating the files or code that changed when a patch was installed. Then, by comparing the patched and unpatched versions of those files, a hacker can examine the specific functions that changed, uncover the vulnerability, and exploit it.

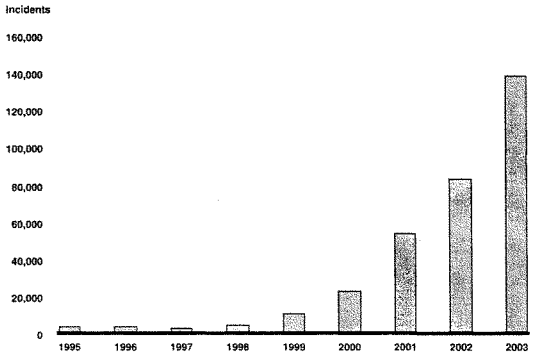
A spate of new worms has been released since February—most recently last month—and more than half a dozen new viruses were unleashed. The worms were variants of the Bagle and Netsky viruses. The Bagle viruses typically included an infected e-mail attachment containing the actual virus; the most recent versions have protected the infected attachment with a password, preventing anti-virus scanners from examining it. The recent Netsky variants attempted to deactivate two earlier worms and, when executed, reportedly make a loud beeping sound. Another worm known as Sasser, like the Blaster worm discussed later, exploits a vulnerability in the Microsoft Windows operating system, while the Witty worm exploits a flaw in certain Internet security software products.

The number of computer security incidents within the past decade has risen in tandem with the dramatic growth in vulnerabilities, as the increased number of vulnerabilities provides more opportunities for exploitation. CERT/CC has reported a significant growth in computer security incidents—from about 9,800 in 1999 to over 82,000 in 2002 and over 137,500 in 2003. And these are only the reported attacks. The director of the CERT Centers has estimated that as much as 80 percent of actual security incidents go unreported, in most cases because

- there were no indications of penetration or attack,
- the organization was unable to recognize that its systems had been penetrated, or
- the organization was reluctant to report the attack.

Figure 2 shows the number of incidents reported to CERT/CC from 1995 through 2003.

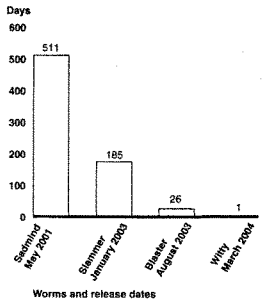
Figure 2: Computer Security Incidents, 1995–2003



Source: GAO analysis based on Carnegie Mellon University's CERT® Coordination Center data.

According to CERT/CC, about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches; however, such patches are often not quickly or correctly applied. Maintaining current patches is becoming more difficult, as the length of time between the awareness of a vulnerability and the introduction of an exploit is shrinking. For example, the recent Witty worm was released only a day after the announcement of the vulnerability it attacked. As figure 3 illustrates, in the last 3 years, the time interval between the announcement of a particular vulnerability and the release of its associated worm has diminished dramatically.

Figure 3: Time Interval between the Announcement of a Vulnerability and the Release of Its Associated Worm



Source: GAO.

Exploited Software Vulnerabilities Can Result in Economic Damage and Disruption of Operations

Although the economic impact of a cyber attack is difficult to measure, a recent Congressional Research Service study cites members of the computer security industry as estimating that worldwide, major virus attacks in 2003 cost $12.5 billion.[9] They further project that economic damage from all forms of digital attacks in 2004 will exceed $250 billion.

Following are examples of significant damage caused by worms that could have been prevented had the available patches been effectively installed:

- On January 25, 2003, Slammer reportedly triggered a global Internet slowdown and caused considerable harm through

[9]Congressional Research Service, *The Economic Impact of Cyber Attacks* (Washington, D.C.: April 1, 2004).

network outages and other unforeseen consequences. As discussed in our April 2003 testimony on the security of federal systems and critical infrastructures, the worm reportedly shut down a 911 emergency call center, canceled airline flights, and caused automated teller machine failures.[10] According to media reports, First USA Inc., an Internet service provider, experienced network performance problems after an attack by the Slammer worm, due to a failure to patch three of its systems. Additionally, the Nuclear Regulatory Commission reported that Slammer also infected a nuclear power plant's network, resulting in the inability of its computers to communicate with each other, disrupting two important systems at the facility. In July 2002, Microsoft had released a patch for its software vulnerability that was exploited by Slammer. Nevertheless, according to media reports, Slammer infected some of Microsoft's own systems. Reported cost estimates of Slammer damage range between $1.05 billion and $1.25 billion.

- On August 11, 2003, the Blaster worm was launched to exploit a vulnerability in a number of Microsoft Windows operating systems. When successfully executed, it caused the operating system to fail. Although the security community had received advisories from CERT/CC and other organizations to patch this critical vulnerability, Blaster reportedly infected more than 120,000 unpatched computers in its first 36 hours. By the following day, reports began to state that many users were experiencing slowness and disruptions to their Internet service, such as the need to reboot frequently. The Maryland Motor Vehicle Administration was forced to shut down, and systems in both national and international arenas were also affected. Experts consider Blaster, which affected a range of systems, to be one of the worst exploits of 2003. Microsoft reported that the Blaster worm has infected at least 8 million Windows computers since last August.

[10]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: April 8, 2003).

- On May 1 of this year, the Sasser worm was reported, which exploits a vulnerability in the Windows Local Security Authority Subsystem Service component. This worm can compromise systems by allowing a remote attacker to execute arbitrary code with system privileges. According to US-CERT (the United States Computer Emergency Readiness Team),[11] systems infected by this worm may suffer significant performance degradation. Sasser, like last year's Blaster, exploits a vulnerability in a component of Windows by scanning for vulnerable systems. Estimates by Internet Security Systems, Inc., place the Sasser infections at 500,000 to 1 million machines. Microsoft has reported that 9.5 million patches for the vulnerability were downloaded from its Web site in just 5 days.

Federal Efforts to Address Software Vulnerabilities

The federal government has taken several steps to address security vulnerabilities that affect agency systems, including efforts to improve patch management. Specific actions include (1) requiring agencies to annually report on their patch management practices as part of their implementation of FISMA, (2) identifying vulnerability remediation as a critical area of focus in the President's National Strategy to Secure Cyberspace, and (3) creating US–CERT.

FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies in prior legislation.[12] In accordance with OMB's reporting instructions for FISMA implementation, maintaining up-to-date patches is part of system configuration management requirements. The 2003 FISMA reporting instructions that specifically address patch management practices include agencies' status on (1) developing an inventory of major IT systems,

[11] A new service to function as the center for coordinating computer security preparedness and response to cyber attacks and incidents.

[12] Title X, Subtitle G—Government Information Security Reform provisions, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L. 106-398, October 30, 2000.

(2) confirming that patches have been tested and installed in a timely manner, (3) subscribing to a now-discontinued governmentwide patch notification service, and (4) addressing patching of security vulnerabilities in configuration requirements.

The President's National Strategy to Secure Cyberspace was issued on February 14, 2003, to identify priorities, actions, and responsibilities for the federal government—as well as for state and local governments and the private sector—with specific recommendations for action to DHS. This strategy identifies the reduction and remediation of software vulnerabilities as a critical area of focus. Specifically, it identifies the need for (1) a better-defined approach on disclosing vulnerabilities, to reduce their usefulness to hackers in launching an attack; (2) creating common test beds for applications widely used among federal agencies; and (3) establishing best practices for vulnerability remediation in areas such as training, use of automated tools, and patch management implementation processes.

US-CERT was created last September by DHS's National Cyber Security Division (NCSD) in conjunction with CERT/CC and the private sector. Specifically, US-CERT is intended to aggregate and disseminate cyber security information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. This free service—which includes notification of software vulnerabilities and sources for applicable patches—is available to the public, including home users and both government and nongovernment entities.

Agencies Are Not Consistently Implementing Common Practices for Effective Patch Management

Common patch management practices—such as establishing and enforcing standardized policies and procedures and developing and maintaining a current technology inventory—can help agencies establish an effective patch management program and, more generally, assist in improving an agency's overall security posture.

Our survey results showed that the 24 agencies are implementing some practices for effective patch management, but not others. Specifically, all report that they have some level of senior executive involvement in the patch management process and cited the chief information security officer (CISO) as being the individual most involved in the patch management process. The CISO is involved in managing risk, ensuring that appropriate resources are dedicated, training computer security staff, complying with policies and procedures, and monitoring the status of patching activities.

Other areas in which agencies report implementing common patch management practices are in performing a systems inventory and providing information security training. All 24 agencies reported that they develop and maintain an inventory of major information systems as required by FISMA and do so using a manual process, an automated tool, or an automated service. Additionally, most of the 24 agencies reported that they provide both on-the-job and classroom training in computer security, including patch management, to system owners, administrators, and IT security staff.

However, agencies are inconsistent in developing patch management policies and procedures, testing of patches, monitoring systems, and performing risk assessments. Specifically, not all agencies have established patch management policies and procedures. Eight of the 24 surveyed agencies report having no policies and 10 do not have procedures in place. Additionally, most agencies are not testing all patches before deployment. Although all 24 surveyed agencies reported that they test some patches against their various systems configurations before deployment, only 10 agencies reported testing all patches, and 15 agencies reported that they do not have any testing policies in place. Moreover, although all 24 agencies indicated that they perform some monitoring activities to assess their network environments and determine whether patches have been effectively applied, only 4 agencies reported that they monitor all of their systems on a regular basis. Further, just under half of the 24 agencies said they perform a documented risk assessment of all major systems to determine whether to apply a patch or an alternative workaround. Without consistent implementation of patch management practices, agencies are at

increased risk of attacks that exploit software vulnerabilities in their systems.

More refined information on key aspects of agencies' patch management practices—such as their documentation of patch management policies and procedures and the frequency with which systems are monitored to ensure that patches are installed—could provide OMB, Congress, and agencies themselves with data that could better enable an assessment of the effectiveness of an agency's patch management processes.

Automated Tools and Services Can Assist Agencies in Performing Patch Management Activities

Several automated tools and services are available to assist agencies with patch management. A patch management tool is an application that automates a patch management function, such as scanning a network and deploying patches. Patch management services are third-party resources that provide services such as notification, consulting, and vulnerability scanning. Tools and services can make the patch management process more efficient by automating otherwise time-consuming tasks, such as keeping current on the continuous flow of new patches.

Commercially available tools and services include, among others, methods to

- inventory computers and the software applications and patches installed;
- identify relevant patches and workarounds and gather them in one location;
- group systems by departments, machine types, or other logical divisions;
- manage patch deployment;
- scan a network to determine the status of patches and other corrections made to network machines (hosts and/or clients);
- assess machines against set criteria, including required system configurations;

- access a database of patches;
- test patches; and
- report information to various levels of management about the status of the network.

In addition to automated tools and services, agencies can use other methods to assist in their patch management activities. For example, although labor-intensive, they can maintain a database of the versions and latest patches for each server and each client in their network, and track the security alerts and patches manually. Agencies can also employ systems management tools with patch-updating capabilities to deploy the patches. This method requires that agencies monitor for the latest security alerts and patches. Further, software vendors may provide automated tools with customized features to alert system administrators and users of the need to patch and, if desired, to automatically apply patches.

We have previously reported on FedCIRC's Patch Authentication and Dissemination Capability (PADC), a service initiated in February 2003 to provide users with a method of obtaining information on security patches relevant to their enterprise and access to patches that had been tested in a laboratory environment.[13] According to FedCIRC officials, this service was terminated on February 21, 2004, for a variety of reasons, including low levels of usage. In the absence of this service, agencies are left to independently perform all components of effective patch management. A centralized resource that incorporates lessons learned from PADC's limitations could provide standardized services, such as testing of patches and a patch management training curriculum.

[13]U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Washington D.C.: September 10, 2003).

Significant Obstacles to Effective Patch Management Remain

Security experts and agency officials have identified several obstacles to implementing effective patch management; these include the following:

- High volume and increasing frequency of patches. Several of the agencies we surveyed indicated that the sheer quantity and frequency of needed patches posed a challenge to the implementation of the recommended patch management practices. As increasingly virulent computer worms have demonstrated, agencies need to keep systems updated with the latest security patches.
- Patching heterogeneous systems. Variations in platforms, configurations, and deployed applications complicate agencies' patching processes. Further, their unique IT infrastructures can make it challenging for agencies to determine which systems are affected by a software vulnerability.
- Ensuring that mobile systems receive the latest patches. Mobile computers—such as laptops, digital tablets, and personal digital assistants—may not be on the network at the right time to receive appropriate patches that an agency deploys and are at significant risk of not being patched.
- Avoiding unacceptable downtime when patching systems that require high availability. Reacting to new security patches as they are introduced can interrupt normal and planned IT activities, and any downtime incurred during the patching cycle interferes with business continuity, particularly for critical systems that must be continuously available.
- Dedicating sufficient resources to patch management. Despite the growing market of patch management tools and services that can track machines that need patches and automate patch downloads from vendor sites, agencies noted that effective patch management is a time-consuming process that requires dedicated staff to assess vulnerabilities and test and deploy patches.

Additional Steps Can Be Taken to Mitigate Risks

As with the challenges to patch management identified by agencies, our report also identified a number of steps that can be taken to address the risks associated with software vulnerabilities. These include:

- Better software engineering. More rigorous engineering practices, including a formal development process, developer training on secure coding practice, and code reviews, can be employed when designing, implementing, and testing software products to reduce the number of potential vulnerabilities and thus minimize the need for patching.
- Implementing "defense-in-depth." According to security experts, a best practice for protecting systems against cyber attacks is for agencies to build successive layers of defense mechanisms at strategic points in their IT infrastructures. This approach, commonly referred to as defense-in-depth, entails implementing a series of protective mechanisms such that if one fails to thwart an attack, another will provide a backup defense.
- Using configuration management and contingency planning. Industry best practices and federal guidance recognize the importance of configuration management when developing and maintaining a system or network to ensure that additions, deletions, or other changes to a system do not compromise the system's ability to perform as intended. Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities, in case usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, accidental loss of files, or major disaster.
- Ongoing improvements in patch management tools. Security experts have noted the need for improving currently available patch management tools. Several patch management vendors have been working to do just that.

- Research and development of new technologies. Software security vulnerabilities can also be addressed through the research and development of automated tools to uncover hard-to-see security flaws in software code during the development phase.
- Federal buying power. The federal government can use its substantial purchasing power to demand higher quality software that would hold vendors more accountable for security defects in released products and provide incentives for vendors that supply low-defect products and products that are highly resistant to viruses.

In addition, DHS and private-sector task forces are taking steps to address patch management. For example, in April, two task forces established by DHS's NCSD and the National Cyber Security Partnership in December 2003 addressed patch management-related issues in their reports. The Security Across the Software Development Life Cycle Task Force recommended that software providers improve the development process by adopting practices for developing secure software.[14] The National Cyber Security Partnership Technical Standards and Common Criteria Task Force advised the federal government to fund research into the development of better code-scanning tools that can identify software defects.[15]

— — — — —

In summary, the ever-increasing number of software vulnerabilities resulting from flaws in commercial software products place federal operations and assets at considerable—and growing—risk. Patch management is an important element in mitigating these risks, as part of overall network configuration management and information security programs. Agencies have implemented effective patch management practices inconsistently. While automated tools and

[14] *Improving Security Across the Software Development Life Cycle*, April 1, 2004.

[15] *The National Cyber Security Partnership Technical Standards and Common Criteria Task Force, Recommendations Report*, April 2004.

services are available to facilitate agencies' implementation of selected patch management practices, several obstacles to effective patch management remain. Additional steps can be taken by vendors, the security community, and the federal government to address the risk associated with software vulnerabilities and patch management challenges. Moreover, OMB's implementation of our recommendations to instruct agencies to provide more refined information on their patch management practices in their annual FISMA reports and determine the feasibility of providing selected centralized patch management services—with which they concurred— could improve agencies' abilities to oversee the effectiveness of their patch management processes.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. Should you have any further questions about this testimony, please contact me at (202) 512-3317 or at daceyr@gao.gov.

Individuals making key contributions to this testimony included Michael P. Fruitman, Elizabeth Johnston, Stuart Kaufman, Anjalique Lawrence, Min Lee, David Noone, and Tracy Pierson.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. PUTNAM. Thank you, Mr. Dacey.

Our next witness is Amit Yoran, the Director of the National Cyber Security Division, Department of Homeland Security. This division provides security services such as cyber space analysis and vulnerability alerts and warnings to both the public and private sector.

Before taking this position, Mr. Yoran served as the vice president of Worldwide Managed Security Services at the Symantec Corp. He also served as an officer in the U.S. military, as the Vulnerability Assessment Program Director for the U.S. Department of Defense's Computer Emergency Response Team and supported security efforts for the Office of the Assistant Secretary of Defense.

He is a graduate of the U.S. Military Academy at West Point and received a Masters of Computer Science from George Washington University.

Welcome to the subcommittee.

Mr. YORAN. Good afternoon, Chairman Putnam and distinguished members of the subcommittee. I am pleased to have an opportunity to appear before this committee to discuss DHS' initiatives focusing on vulnerability management.

Today's infrastructures' interdependence on computer and control systems represents significant challenges in managing system risk. Many vulnerability management efforts can be characterized as a cat and mouse game of discovery, system patching, exploitation and incident response. We have several efforts well underway to best leverage Federal resources and collaborate with the private sector. While I am proud of our efforts to date, I also recognize that this is only the very beginning of an ever maturing process. My experiences continue to strengthen my conviction that fundamental changes in software and hardware architecture are required for us to break out of this cat and mouse cycle and change the fundamental paradigms of cyber security.

A major element of successful vulnerability management include dynamic 24–7 situational awareness capabilities and the mechanisms for response. The Department of Homeland Security in partnership with Carnegie Mellon University's CERTCC has created the U.S. CERT to serve as a national focal point for response and partnership among and between public and private sectors. Already the U.S. CERT has created a national cyber alert system.

Only through an active and productive working relationship with the private sector can we hope to achieve the type of situational awareness necessary and core capability required for our Nation to respond and recover from cyber incidents. To that end, U.S. CERT has over the past few months developed coordination activities and 24–7 interactions with the operational elements of the 14 ISACs of our Nation's critical infrastructures. We are actively growing these relationships to foster trust and gain a better appreciation for one another's capabilities, relative strengths, and understanding for how we might be able to work together during time of crisis. This initial operational interaction with the ISACs has been very warmly received and represents a fundamental building block for the public/private partnership.

We have also increased our efforts interacting with cyber experts in the private industry who might be able to provide great value

to the Nation in interpreting cyber activities as they unfold. I commend those entities in the private sector which have already stepped up to the plate in helping the U.S. CERT in this ongoing and collaborative effort.

It is our goal that this will result in a more structured partnership program this summer. The U.S. CERT Partner Program will become the cornerstone of national cyber security coordination for preparedness, analysis, warning and response efforts across the public and private sectors. Such a partnership and early warning network has already been specifically called for by the National Cyber Security Partnership's Early Warning Task Force recommendations and other advisory bodies and entities.

The U.S. CERT is developing a focused control system center to specifically look at cyber vulnerabilities, exploits, protective measures and coordinate response activities within the critical infrastructure control systems. This Control System Center will work with the control systems and SCADA vendor communities, ISACs and operators to increase awareness of and attention to security considerations in the operation of our Nation's critical infrastructures. The Control System Center will also include the development of a control system test bed facility.

Over the past 3 months, we have helped the public sector better organize itself in the area of cyber security, first, through the creation of the Government Forum of Incident Response and Security Teams. Those individuals and organizations responsible for cyber incident response within the Federal community are sharing information and better coordinating their defensive efforts. Second, we have created the Chief Information Security Officer Forum for the CISOs of the Federal Government to share common experiences, challenges, techniques, programs and capabilities. Those CISOs, the operators responsible for securing the information systems in the Federal Government, have specific efforts underway in the areas of FISMA, patching and configuration management and incident reporting and response.

In addition to helping the Government better secure its cyber space, we are preparing the Federal Government to bring its resources to bear in a more coordinated fashion during time of cyber crisis. Through the creation of the Cyber Interagency Incident Management Group, departments and agencies with significant security operating capabilities and authorities to operate in the cyber realm are already preparing coordinated Federal action.

The efforts I have mentioned constitute only a portion of the national programs underway, not only within the Department of Homeland Security and the Federal Government but most importantly within the private sector to address cyber vulnerabilities. While these efforts are improving our preparedness, the most effective step toward vulnerability management must occur through the prevention step. A clear focus on improved software assurance must become a cornerstone for the public/private partnership. The Software Assurance Task Force of December's Cyber Security Summit has made numerous specific recommendations to improve the quality of code throughout the software development life cycles. Those recommendations and others underway are fundamental for the private sector to mitigate risks and assure software integrity,

reducing the numbers and impact of vulnerabilities we will face in the future.

Industry leaders such as Microsoft and others have enhanced their development processes. Their adoption of best practices may lead to a decline of vulnerabilities in server software and corresponding reduction in the number of patches for their customers. Oracle and others are committed to more secure products and have undergone numerous security evaluation efforts of their products. We commend those who are making security improvements a clear priority for their development practices and for their business.

Thank you for the opportunity to testify before you today and I would be happy to answer any questions you may have at this time.

[The prepared statement of Mr. Yoran follows:]

Statement by
Amit Yoran
Director, National Cyber Security Division, Office of Infrastructure Protection
U.S. Department of Homeland Security
"Information Security – Vulnerability Management Strategies and Technology"

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
Committee on Government Reform
U.S. House of Representatives
June 2, 2004

Good afternoon, Chairman Putnam and distinguished Members of the Subcommittee. My name is Amit Yoran, and I am Director of the National Cyber Security Division of the Office of Infrastructure Protection in the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate. As we approach the National Cyber Security Division's one-year anniversary, I am pleased to have an opportunity to appear before the committee again to discuss "Information Security – Vulnerability Management Strategies and Technology." In the National Cyber Security Division (NCSD) of DHS, we have designed and implemented our programs to execute against various key cyber security issues for the Nation, including those laid out in the *National Strategy to Secure Cyberspace* ("the Strategy"). Vulnerability management, reduction, and assessment are an integral part of all aspects of our strategy, and span across all program areas within the Office of Infrastructure Protection and the NCSD. Our initiatives are focused on the areas of incident management, our on-going collaboration with the public and private sectors, software assurance, and vulnerability assessment. As the focal point for the public and private sectors on cyber security issues, we work closely with our interagency colleagues and private sector partners to address these critical components of the mandate to increase our Nation's cyber security and improve our ability to mitigate vulnerabilities to the greatest extent possible.

Introduction

The National Cyber Security Division (NCSD) was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues. NCSD is charged with coordinating the implementation of the *National Strategy to Secure Cyberspace* released by the President in February 2003. Since our creation, we have been evaluating and securing our areas of greatest vulnerability, in partnership with private industry.

DHS is working closely with our partners in the federal government, the private sector, and academia on a variety of programs. DHS recognizes that each entity may

bring unique capabilities, responsibilities, and/or authorities to bear on cyber security issues. We recognize that the challenge of securing cyberspace is vast and complex, that threats are multi-faceted and global in nature, and that our strengths – and our vulnerabilities – lie in our interdependencies. Further, the cyber environment in which the world operates is constantly changing. We recognize that information sharing and coordination are crucial to improving our overall national and economic security. Cognizant of these realities, our cyber security initiatives are designed to address each of the priorities set forth in the *National Strategy to Secure Cyberspace* ("the Strategy"):

Priority I:	A National Cyberspace Security Response System
Priority II:	A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III:	A National Cyberspace Security Awareness and Training Program
Priority IV:	Securing Government's Cyberspace
Priority V:	National Security and International Cyberspace Security Cooperation

Our cyber security programs address each of these priorities and are beginning to improve our ability to manage vulnerabilities and incidents.

Vulnerability Management

The highly interconnected and interdependent digital economy in which we live and work today presents many challenges to managing information system vulnerabilities in all spectrums of the Nation including: government, large and small companies, academia, and even our private homes. The proliferation of complex information systems and the speed with which information flows today present great challenges for developing and coordinating programs to manage those vulnerabilities on the one hand, while also disseminating the appropriate information to those who need it, on the other. NCSD has initiated several programs to coordinate with various stakeholders, manage collaborative efforts, and address the diverse owner, operator, and user communities.

Incident Management

A major element of successful vulnerability management is incident management that includes a 24/7 incident management capability and the ability to know what to do when vulnerabilities are identified. Successful incident management also requires strong information sharing, communication, and coordination capabilities. DHS has implemented several initiatives aimed at addressing these different aspects of incident management.

Priority IV of the Strategy gives DHS the responsibility for securing government's cyberspace. The U.S. Government has been actively engaged in assessing our preparedness and processes for responding to cyber incidents. In October of 2003, DHS participated in the first national cyber-focused exercise, called "Livewire," which

provided a baseline for the federal government incident response capability and communication paths. Livewire also directly supported the creation of the Cyber Interagency Incident Management Group (Cyber IIMG), which was developed to improve response procedures and capabilities across government agencies. The Cyber IIMG coordinates intra-governmental preparedness and operations to respond to, and recover from, cyber incidents and attacks. The group brings together senior officials from DHS, the White House, the National Security Council, Homeland Security Council, OMB, law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security capabilities. The collaboration of these agency officials provides an improved capability to analyze and coordinate a national level response to incidents that may impact cyber assets. In addition to the ability to focus portions of their agencies' resources, they possess the necessary statutory authority to take decisive actions in response to incidents. The Cyber IIMG meets on a regular basis to address cyber incident coordination in general and identifies specific areas of concern to focus on at each meeting.

In addition to the coordination of senior management in the Cyber IIMG, DHS has also established the Government Forum of Incident Response and Security Teams (GFIRST), a consortium of federal response and information security teams working together to bolster government-wide incident response capabilities. This group provides a forum for security-focused technologists to communicate with a trusted set of peers responsible for protecting the government-owned and operated elements of the Nation's critical infrastructure. GFIRST promotes cooperation among the full range of federal agencies, including defense, civilian, intelligence, and law enforcement. We are already seeing the benefits of both the Cyber IIMG and GFIRST in improving communication and coordination among government agencies toward incident preparedness and response efforts.

DHS, in coordination with the White House and other federal agencies, has been working to provide mechanisms for improving vulnerability management and incident response that are crucial to protecting the Nation from a variety of vulnerabilities and attacks. DHS is developing a National Response Plan (NRP) that will include a Cyber Annex outlining the Government's processes for responding to a cyber attack or incident. The NCSD is developing the Cyber Annex to ensure that there are robust, reliable and efficient mechanisms for managing national level cyber incidents.

Congress also contributed greatly to the impetus and ability of federal agencies to protect their information infrastructure by passing the Federal Information Security Management Act of 2002 (FISMA). FISMA has been a key component in vulnerability mitigation and cyber preparedness by providing a framework for enhancing the effectiveness of information security and vulnerability management in the federal government. That framework has become a very visible federal agency information security benchmark, and as such, it has served to accelerate agencies' deployment of automated, enterprise-wide security assessment and security policy enforcement tools as well as threat and vulnerability management tools. FISMA also calls for the operation of a central Federal information security incident center. The Federal Computer Incident

Response Center (FedCIRC) program fulfilled the functions specified under FISMA and today, those functions are fully supported and integrated into NCSD watch operations. NCSD continues to maintain close coordination with the Office of Management and Budget (OMB) on cyber events that may impact the Federal government. DHS is a strong advocate of FISMA as an important, cohesive platform to secure government cyberspace.

Aside from our government-focused initiatives, DHS established the U.S. Computer Emergency Readiness Team (US-CERT) as its overall cyber security operational entity. US-CERT represents a partnership between NCSD and the public and private sectors, the founding partnership of which is between the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University. US-CERT provides a national coordination center that links public and private readiness and response capabilities to facilitate information sharing across all infrastructure sectors and helps to protect our Nation's cyber infrastructure. The overarching objective of US-CERT is to facilitate and implement a systematic readiness, coordination, and response mechanism to address cyber incidents and attacks across the United States, as well as to mitigate the cyber consequences of physical attacks.

The National Cyber Alert System (NCAS), launched by US-CERT in January of this year, is an important mechanism for vulnerability and incident management and warning. The NCAS is an operational system that delivers targeted, timely, and actionable information to Americans to allow them to secure their computer systems. Information provided by the system is designed to be understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. The NCAS provides general guidance for users and the ability to reach millions of users at once. The information NCAS provides is crucial to helping Americans take appropriate preventative measures against vulnerabilities to protect their computers.

When US-CERT has vendor-specific vulnerability or threat information rather than more general information typically sent through the NCAS, we communicate directly with the individual company when possible. The recent Cisco vulnerability is an important example of how we communicated – and collaborated – with the private sector on a vendor-specific vulnerability. US-CERT was notified by Cisco Corporation that there was a vulnerability in the Cisco Internetwork Operating System (IOS) implementation of the Simple Network Management Protocol (SNMP). This vulnerability affected many versions of the IOS and could have resulted in a sustained denial of service (DoS) condition if it had been exploited. Cisco representatives requested US-CERT assistance in providing the broadest possible dissemination of information concerning this vulnerability. The US-CERT incident management team was notified immediately and began efforts to coordinate notification of this issue. The US-CERT issued a Technical Cyber Security Alert using the NCAS and, utilizing the HSIN (Homeland Security Information Network)/US-CERT Portal, notified many cyber security communities, including the federal Chief Information Security Officers, the Information Sharing and Analysis Centers (ISACs), and critical infrastructure owners and operators, of the emergence of this new vulnerability. The ability to communicate with

specific companies in such cases to manage the vulnerability and the subsequent mitigation efforts is crucial and is one of the key drivers behind the creation of the US-CERT Partner Program.

The US-CERT Partner Program

DHS is currently working closely with the private sector to develop a comprehensive operational partner program to increase the Nation's cyber security. The US-CERT Partner Program will establish a formal collaboration mechanism between DHS, other government entities, academic institutions, and the private sector. This program will focus on partnerships between the public and private sectors for the purpose of improving national situational awareness with regard to cyber security and will coordinate cyber security across Federal, State, Local government, academia, and private industry. The Partner Program will be the cornerstone of national cyber security coordination for preparedness, analysis, warning, and response efforts across the public and private sectors to help ensure the cyber security of our national critical infrastructures and the Internet. Program partners will include the spectrum of the critical infrastructure sectors (including the Information Sharing and Analysis Centers (ISACs), industry associations, etc.), and the organizations that support these sectors from the private and public sectors, the research community, and academia.

The mission of the US-CERT Partner Program is to bring about measurable improvement in the Nation's ability to prepare for, recognize, respond to, and recover from cyber security incidents. In order to carry out this mission, the US-CERT Partner Program's objectives are to:

- Share information to prevent, predict, detect, and respond to cyber threats and vulnerabilities;
- Increase emphasis on improving the cyber security of our Nation's critical infrastructures;
- Provide actionable identification, analysis, and warning of cyber vulnerabilities, malicious code, exploits, and viruses to member partners;
- Improve cyber event response coordination within and between public and private sectors;
- Ensure a secure and trusted forum to promote analysis and facilitate exchange; and
- Create an effective forum to demonstrate national commitment to cyber security.

In order to provide actionable identification, analysis, and warning of cyber vulnerabilities, malicious code, exploits, and viruses to member partners, the US-CERT Partner Program will create a mechanism to collect, analyze, remediate, and disseminate information pertaining to the protection of our Nation's critical infrastructures, including vulnerabilities. Partners will commit to take steps to increase our overall cyber security preparedness, and our collaborative efforts will lead to improved vulnerability

management and incident response, and thus increased national and organizational cyber security.

Software Assurance

Another facet of successful vulnerability management is the importance of addressing and reducing vulnerabilities from the beginning. Thus, software development and assurance is a fundamental area of focus for DHS and for the public-private partnership.

The NCSD is taking a proactive approach to software assurance by examining problems such as flaws, bugs, and backdoors. Additionally, the NCSD is examining ways to improve the effectiveness, reliability, and risk of patches and software configuration. By addressing the root problems of current software development, we can eliminate vulnerabilities before products and application systems are deployed.

The NCSD recognizes the importance of creating more robust software security so that all users can continue to derive value from current and future software products. DHS is developing a program plan to work closely with the private sector, academia, and other government agencies to produce better quality and more secure software. DHS is evaluating the software development lifecycle, including people, process, procedures, and technology to implement a collaborative effort to mitigate risks and assure software integrity.

- **People** – Focuses on software developers (includes education and training) and users
- **Processes** – Focuses on developing best practices and practical guidelines for the development of secure software and associated standards, specifications, acquisition language
- **Technology** – Focuses on software evaluation tools

This comprehensive approach is consistent with recommendations from the Security Across the Software Development Lifecycle Task Force of the Cyber Security Partnership formed in connection with the National Cyber Security Summit that was co-sponsored by DHS and industry in December 2003. Through the work of the task force and individual corporate efforts, the private sector is seriously engaged in this effort. Companies are committing to reducing vulnerabilities by using state of the art engineering practices, standards, and processes throughout the cycle of creating their software. For example, a software vendor tells us that such enhanced development processes have resulted in a notable decline of vulnerabilities in some of their server software and a corresponding reduction in the number of patches for their users.

Furthermore, research and development (R&D) must play a significant part in enhancing cyber security for the future. The DHS's Science and Technology (S&T) Directorate has plans for R&D investments aimed at improving software assurance and code development, as part of programmatic activities that will be initiated later this fiscal

year. In addition, the S&T Directorate has initiated an effort aimed at supporting the creation of large-scale data sets for testing of network security technologies. These data sets are intended to support the university and industry R&D communities by improving research, development, and evaluation of alternative approaches to network security.

Technology

Chief information security officers play a vital role in vulnerability management for their organizations. As such, DHS established the Chief Information Security Officer Forum (CISO Forum) for the education and professional development, collaboration, and coordination venue for agencies' designated senior federal IT security executives. The CISO Forum provides a trusted venue for our government information security officers to collaborate and share effective practices, initiatives, capabilities, successes and challenges. In addition, the CISO Forum provides education on FISMA and leading edge security tools and methodologies – including encryption, authentication, shielding, configuration management, and intrusion detection. The education and interagency collaboration in the CISO Forum allows federal chief information security officers to continually improve vulnerability management in their respective agencies and departments and better secure federal systems.

We hear much about patch management as we look toward vulnerability mitigation possibilities. Since the Patch Authentication and Dissemination Capability (PADC) program was initiated in 2001, patch management technology has significantly surpassed the spartan capability of that time. In an effort to streamline its own efforts in this regard, the NCSD discontinued the PADC program. It was determined that the existing contract was too inflexible and financially constrained to affect necessary enhancement. Since the management, architecture, and resources of each agency vary, it is unlikely that a single solution will satisfy every need. Therefore, NCSD has engaged the CISO Forum to undertake an examination of agencies' needs, as well as the current state and future development of patch technology. A CISO Forum working group will study current patch technology and attempt to understand the common needs of agencies, in addition to how the patch management industry may assist in responding to sudden and potentially damaging exploitation of vulnerable software. Additionally, with the implementation of the National Cyber Alert System, discussed previously, US-CERT will fill the void of early notification of vulnerabilities that the PADC program provided. Patch management is necessary to address the vulnerabilities and incidents that occur due to today's software security limitations. DHS is striving for the proliferation of secure software for consumers and other customers through our software assurance programs and efforts with software developers. Until that time, however, effective patch management is a necessary objective.

Vulnerability Assessment

Comprehensive vulnerability assessment is another necessary aspect of vulnerability management. As part of the Critical Infrastructure Protection initiative

mandated under Homeland Security Presidential Directive 7 (HSPD-7), released by President Bush on December 17, 2003, the Department of Homeland Security is coordinating physical and cyber vulnerability assessments of critical infrastructures, working with sector specific agencies. Under HSPD-7, sector specific agencies have responsibility to identify critical assets, develop methodologies to assess vulnerabilities, and map those vulnerabilities to critical assets in a risk assessment analysis. DHS is responsible for the correlation, analysis, and trending of the information provided by those agencies. The NCSD, as the information technology (IT) sector specific lead agency, is responsible for identifying the critical assets and related vulnerabilities in the IT sector.

A fundamental goal of the National Critical Infrastructure Protection (CIP) Program is to identify and protect infrastructures that are deemed most "critical" in terms of national-level public health and safety, governance, economic and national security, and public confidence. The Department of Homeland Security (DHS) recognizes that such protection requires the cooperation and essential collaboration of federal agencies and departments, state and local governments, and the private sector. Accordingly, to achieve the overarching goal of protection, and to reduce vulnerabilities across the entire critical infrastructure – physical and cyber - DHS is coordinating the development of consistent, sustainable, effective, and measurable CIP programs across the federal, state, local, and private sector. DHS is coordinating with SSAs in developing their plans for implementing critical infrastructure protection (CIP) responsibilities required under Homeland Security Presidential Directive (HSPD) 7. These Sector-Specific Plans will be incorporated into the NIPP, called for under Paragraph 27 of HSPD-7.

After the initial assessment and determination of vulnerabilities by all sector specific agencies, a remediation plan will be developed within each sector specific agencies to address the vulnerabilities. DHS, NCSD will analyze the inputs and look for common vulnerabilities which can be addressed through long-term strategic initiatives. These efforts will vastly improve vulnerability mitigation and management in the 13 critical infrastructure sectors.

Conclusion

DHS has made great strides to implement a variety of programs and partnerships to help secure cyberspace. Vulnerability management is a critical area targeted by DHS in order to increase cyber security not only for today but also for the future, including comprehensive incident management initiatives, coordination with the private sector through the US-CERT Partner Program, software assurance and development programs, and cyber vulnerability assessments of the critical infrastructure sectors. In addition, we bring together key cyber security stakeholders together through various forums to address the technical and management issues in a collaborative way across the federal government, state and local governments, academia, and the private sector.

Thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.

Mr. PUTNAM. Thank you, Mr. Yoran.

Our next witness is Dawn Meyerriecks, the Chief Technology Officer, Defense Information Systems Agency and provides technical direction for Defense's Global Information Grid initiative. Before joining DISA in September 1995, Ms. Meyerriecks was the Chief Architect for the Army Global Command and Control System.

She attended Carnegie Mellon University and was awarded a Bachelor of Science Degree in electrical engineering with a double major in administration and management science. She has also received a Master of Science in computer science from Loyola Marymount University. Her awards include InfoWorld 2002 CTO of the Year; Federal Computer Week 2000 Top 100; and the Presidential Distinguished Service Award in November 2001.

Welcome to the subcommittee. You are recognized.

Ms. MEYERRIECKS. Thank you, Mr. Chairman. It is my privilege to testify for this august body on vulnerability management in the Department of Defense today. You do have handouts of slides and I would like to speak to those. Because we actually put some statistics and reporting on ourselves, it would probably be useful for you to glance at those as we go through the presentation.

Let me start with slide 2 to explain where DISA sits in terms of the Department of Defense. We are the IT integrator, we are the joint acquisition, engineering and operations organization within the Department of Defense and 50 percent of our 8,000 personnel are deployed to the field at any particular point in time. If you look at that particular slide, we put in the wide area networks, we run the computing centers and we also build the applications stack for joint command and control and joint combat support operations, as well as a number of other things we do on the righthand side of the slide. We do White House communications support to the President and a number of related computer science and electrical engineering systems engineering things that actually pull the whole capability together as the backbone infrastructure that supports the Department of Defense. I thought that was important to go through that to give you kind of where we sit in terms of DOD responsibilities.

If you will move with me to the next slide on incidents reported, you can see by the curves that some interesting things are happening. The initial curves are related to the fact that this is kind of a relatively new sport but also that we got better in terms of detection. You see fairly steep curves in terms of year over year, 1997 to 2002. You will notice that it flattened a bit between this year and last year and we attribute that, based on ongoing analysis, the fact that we have tightened our NPPR net/Internet gateways. Our NPPR net is the DOD's intranet, if you can envision it as our corporate intranet, and we actually tightened up a great deal of the protocols that we make available to the Internet community in terms of the kinds of traffic that we pass. At least so far that looks like that has been a very key strategy for us. It is a big part of our Defense in-depth approach. I wanted to highlight that as we move into the vulnerability management and talk about the servers and computers in the department that we don't count on any one of these in order to address the problem, we actually are put-

ting in checks and balances in as many places as we have opportunity.

On the next slide, I am going to drill down on the two sorts of most onerous access problems we see from a computer perspective. We have a whole categorization that we have worked across the community and we are going to spend a little time assuming with you are familiar with unauthorized root access and unauthorized user access, let me give you two examples. Unauthorized root access in a command and control application would say that somebody who achieved that could actually change the position of friendly or enemy forces anyplace on the planet if they were at the right server, pretty onerous for us. Unauthorized user access would say that if I were the actual track manager for my position in terms of the ship if I am on ship, I could only change that particular piece for which I have legitimate access. Those are the two sorts of things we worry about most in terms of impact to mission.

If you will turn with me to the next slide which is serious incidents in DOD, if you keep in mind those two situations then you can see the graphs. It is a relatively busy slide but I will tell you the trend for user level access is slightly downward if we smooth those curves. The trend for CAT1 root or administrator access is slightly upward if we smooth those curves. The good news is that overall this represents 4 million computers in the unclassified environment that the DOD supports and the number of incidents actually relates to the number of computers that have been compromised at that level. So the good thing is in orders of magnitude, clearly 35 is still something to be worried about given the magnitude of the work that we do.

If you will turn to the next slide, No. 6, why did these attackers succeed, I think we have shown these slides in the past or similar slides that match the statistics my colleagues have spoken to, 90 percent, based on the data we collect and we run the DOD CERT, are preventable. You can see the progress we are making there in terms of 26 percent of those we actually are ahead in terms of having issued an information assurance vulnerability alert to the department that people are required to act on within prescribed time constraints and the 64 percent my colleagues have talked about in terms of misconfigurations and the configuration management point you made in your opening statements, there is still 10 percent that we can't predict and that we deal with as they occur.

If you will turn to the next slide, this is a pretty simplistic statement of what it is we are trying to do. We try to put these out so that it is very simple for folks to follow what their job is particularly our system administrators and our operators, those charged with protecting the IT assets of the Department.

This will be my final slide, steps to the goal, there are drilled down slides that are provided further in the brief that talk to each one of these points. We have done a couple of things this year that I think are very important that we articulate. One is we have put in place a clear chain of command. There is a single belly button now that is responsible for the status of the IT infrastructure in the Department. It is a four star and we are a component of supporting that four star. His or her responsibility today is to monitor, manage and operate the network and the associated IT assets.

The steps to the goal, the preventive, proactive piece, we have put together secure configuration guidance in concert with the National Security Agency and we make those broadly available. We have had some success with actually getting vendors in step two to ship us products that are configured from their factories that are in compliance with that secure guidance so that we actually get components from the factory that are already configured accordingly. We also distribute gold disks for those that want to start from scratch with computers that are not configured that way and provide antivirus software and enterprise level not just to the Department in terms of IT assets that we own but also for home computer use. We find a lot of times one of the problems is people bring in disks that are actually infected. That way we can preclude some of that.

Step three, we have a very robust set of patch servers stood up not only on our intranet but also on our classified network so we can keep current. We have the IAVA process I talked to and we are in the process of procuring for the Department and automated remediation tool so that we can take inventory and apply patches as they become available as it makes sense to do so.

Step four is the state of all the computers we have in the process of this procurement but we also send out compliance teams that do on the order of several hundred visits a year and we are training the services to be able to do this themselves as well. We also spot check that people are keeping their configurations current.

With that, I am happy to take any questions the committee has.

[The prepared statement of Ms. Meyerriecks follows:]

NOT FOR PUBLICATION UNTIL RELEASED BY THE
GOVERNMENT REFORM SUBCOMMITTEE, TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

WRITTEN STATEMENT OF

MS DAWN MEYERRIECKS, CHIEF TECHNOLOGY OFFICER, DEFENSE
INFORMATION SYSTEMS AGENCY

BEFORE THE
GOVERNMENT REFORM SUBCOMMITTEE ON TECHNOLOGY, INFORMATION
POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

WEDNESDAY
2 JUNE 2004

CLEARED
FOR OPEN PUBLICATION
MAY 2 5 2004 8
SECURITY REVIEW
DEPARTMENT OF DEFENSE

NOT FOR PUBLICATION UNTIL RELEASED BY THE
GOVERNMENT REFORM SUBCOMMITTEE, TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

DFOISR 04-C-0222
TOTAL P.02

STATEMENT FOR THE RECORD
MS DAWN MEYERRIECKS
DEFENSE INFORMATION SYSTEMS AGENCY
BEFORE
GOVERNMENT REFORM COMMITTEE
TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS SUBCOMMITTEE

Prepared Statement of Ms Dawn Meyerriecks, Chief Technology Officer, Defense Information Systems Agency, before the Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Washington, D.C., June 2, 2004.

Thank you, Mr. Chairman and members of the Subcommittee, for this opportunity to testify before your Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census on the subject of Information Security – Vulnerability Management Strategies and Technology. I am Dawn Meyerriecks, Chief Technology Officer for the Defense Information Systems Agency (DISA).

As Chief Technology Officer for the Defense Information Systems Agency, I, along with Lieutenant General Harry D. Raduege, Director of DISA, am responsible for guiding the Agency's technical direction to execute the Global Information Grid (GIG) Initiative. I am responsible for the identification, evaluation, and incorporation of technology into the Agency's business processes and products.

DISA is a combat support agency. DISA is responsible for building, operating and protecting joint command, control, communications, and computer capabilities to help catalyze and sustain the Department of Defense's (DoD) transformation from platform-centric to network-centric operations. Key to this transformation is the foundation infrastructure known as the Global Information Grid (GIG).

The GIG is a network of unprecedented complexity. It crosses organizational boundaries within DoD and many outside of DoD. The GIG is composed of a huge variety of computer, software, and communications technologies. The responsibility for managing these technologies is currently fragmented across many DoD organizations and extends to many of our commercial partners. In order to better align the management of the GIG with DoD operational priorities, and to improve management and accountability, DoD is implementing a concept called NetOps, or network operations. One facet of NetOps is the development of a clear chain of command for the GIG, starting with U.S. Strategic Command. Accountability and reporting for vulnerability management in the DoD will be handled in this chain.

Assuring the availability of the GIG, and assuring the execution of missions that depend on the GIG are the key principles of DoD information assurance. DISA believes that security in the GIG can only be built and maintained by a broad DoD effort to design security into the GIG; to maintain this security as conditions change; to train our people to perform secure operation of the GIG; and then to operate the GIG in a way that ensures mission effectiveness for the DoD, even in the face of cyber attack.

DoD resists cyber attack by employing a multi-layered defense strategy. Core to this strategy is the notion of vulnerability management. Vulnerability management is a process that includes the development of DoD standards for secure configuration of devices in the GIG; the deployment of these configurations to every GIG component; the development and deployment of modified configurations, including patches, as new vulnerabilities and attacks are discovered and developed; and the local and global auditing and reporting of compliance with the DoD configuration standards.

DISA has coordination, strategy development, technology acquisition and fielding, auditing, and operations roles in vulnerability management. I'll talk about the DISA operations roles first, then talk about some of our technology acquisition and deployment efforts, and conclude with our auditing and verification efforts.

The DISA Global Network Operations and Security Center (GNOSC) performs and oversees the essential network and systems management of the GIG on a 24 by 7, 365-day a year basis, to ensure sustained and responsive, integrated network operations. The GNOSC is the single network operations center in DoD with a composite view of unclassified and classified global voice, data, and video communications used for command and control. Its primary mission is to direct, manage, control, monitor, protect, and report on essential elements and applications that comprise the GIG.

The DoD Computer Emergency Response Team (DoD-CERT) is charged with the global analysis of real or potential network security threats to the GIG. In partnership with the GNOSC, the DoD-CERT protects, defends, and restores the integrity and availability of the essential elements and applications that comprise the GIG under the full spectrum of conflict. An important vulnerability management role of the DoD-CERT is to monitor and research emerging vulnerabilities and attacks. When necessary, the DoD-CERT alerts all in DoD of the need to react, often by changing the standard configuration of a device. These alerts are called Information Assurance Vulnerability Alerts (IAVA) and have been issued since 1998. I will talk a bit more about IAVA later in my testimony.

The GNOSC and DoD-CERT provide primary support to the Joint Task Force-Computer Network Operations (JTF-CNO), a component of U.S. Strategic Command. As part of its larger DoD NetOps mission, the JTF-CNO oversees, coordinates, and directs information assurance

operations throughout the Department. Since the late 1990's the JTF-CNO has successfully defended DoD networks, thus ensuring the continuity of DoD operations in the face of computer intruders, viruses, and worms. The JTF-CNO's role in vulnerability management includes oversight of the IAVA process, and the collection and reporting of statistics on how well DoD organizations are doing in deploying and maintaining secure configurations.

Now I'd like to talk about DISA's efforts to develop the right, secure configurations for DoD, and our efforts to deploy technology that makes the complete cycle of vulnerability management more certain.

The innermost layer of our DoD cyber defenses is the computer itself. Ensuring each computer is configured securely and that each stays configured securely as conditions change seems like a simple problem, but it has been a tough one to solve for both DoD and industry. Many factors contribute to the complexity of this goal. These include: the intricacies of configuring a modern operating system securely; the difficulty in knowing that once configured, it is configured correctly; the sheer volume of new vulnerabilities in many operating systems; the increasing numbers of systems that need to be maintained; and the difficulty in updating and verifying the security of each of these machines in response to each new vulnerability. To help emphasize this point, there are currently more than 6,000 unique vulnerabilities listed in the Common Vulnerabilities and Exposures dictionary, the industry-accepted list of standard names for vulnerabilities that is maintained by the MITRE Corporation.

Despite these complexities, the first step on the path is clear: define secure configurations for DoD computers. Today's operating systems and applications are more flexible than ever, making the configuration possibilities practically infinite. The good news is that we have had success with innovative government and industry partnerships in developing

best practices in operating system and application configuration. An example is the partnership among DISA; the National Security Agency; the non-profit Center for Internet Security (CIS); the General Services Administration; the National Institute of Standards and Technology; Microsoft; and the Systems, Audit, Network, and Security Institute (generally known as the SANS Institute). This partnership resulted in consensus security configuration documents for Microsoft Windows that are published inside the DoD as Security Technical Implementation Guides (STIG), and are also published by NIST and by the CIS. Commercial Microsoft Windows systems administration training is now available that teaches to the standards defined in these guides, and finally, some major computer vendors have indicated interest in shipping computers pre-installed with these configurations and at least one is doing so. Since configuring a system to the DoD standard can be labor intensive and prone to error, the potential benefits to the Department are significant if vendors deliver products already properly configured.

Through similar collaborative processes, we have developed guides for every prevalent operating system and major application in use in the DoD; many are also applicable to the rest of the federal government. These community processes have laid the groundwork; we now have an established community consensus on operationally stable and secure configuration baselines.

The next step is to deploy these configurations everywhere in the Department. Currently we depend primarily on configuration by system administrators. This can be slow and prone to error, even when the system administrator has tools to help push clones of properly configured software out to many machines. Therefore, a DoD goal is to make deployment of the secure configurations more simple and reliable. One way is to urge software and hardware vendors to include the configurations when shipping products to the Department. We believe this is ultimately a large part of the answer to the problem of initial configuration of machines to proper

standards.

Another aid to the configuration of machines to the DoD standard is a DISA-developed product known as the Gold Disk, which is based on the standard configuration guidance. This government-developed product is intended to help system administrators determine the configuration of a computer and then help them automatically fix most configuration vulnerabilities. In calendar year 2003, we provided this technology to DoD for key Windows operating system versions and we are developing versions for some UNIX environments.

In a perfect world, we would be finished once we had the machines configured properly. However, with systems development and the installation of new systems and software, our infrastructure and systems are constantly changing. With change come new opportunities for our enemies to exploit our vulnerabilities. More importantly, with the worldwide usage and sheer complexity of common operating systems and applications, developers, users, researchers, and hackers frequently discover vulnerabilities. As each new vulnerability is identified, software vendors mount a rapid effort to understand the ramifications of the vulnerability and to develop a fix that removes or at least minimizes the vulnerability. Often, the vendors issue a short-term fix in the form of a patch to their existing software and then incorporate a design change in later versions of their software. However, no matter who first identifies a new vulnerability, the information about the vulnerability often becomes widely known in a matter of days. Therefore, a critical component of vulnerability management in DoD is to keep operating systems and application configurations up-to-date with the latest vulnerability patches as they are released. The challenge we face is not only to counter future attacks through installed defenses, but also to develop processes and tools to maintain the secure state of our systems, both as a matter of course and as new threats emerge.

As mentioned earlier, DoD has implemented a process called IAVA to mandate the application of these short-term fixes for software and configurations when a significant threat to DoD missions exists. The IAVA process requires the Combatant Commanders, Services, Defense Agencies, and Field Activities to update configurations to incorporate the new patches or to take other vulnerability remediation actions directed by the DoD-CERT and to report their compliance, so the JTF-CNO can determine overall DoD risk.

Application of patches or other configuration changes to many machines quickly is the crux of the vulnerability management problem. DoD has not fully solved this part of the problem, but we have taken significant steps to make configuration change easier and more certain. DISA has established a distribution system for the dissemination of security relevant patches throughout the DoD. Patch repositories and anti-virus distribution servers are available on the classified and unclassified GIG networks. These repositories enhance DoD's ability to protect against newly announced vulnerabilities because we are no longer competing with the entire Internet community for access to vendor-released patches. DoD users have exclusive access to the repositories, thus speeding up the overall response. From this foundation, we have established DoD Software Update Service (SUS) Servers on the unclassified and classified networks, for the Microsoft baselines. These SUS Servers provide DoD system administrators with automatic notification, and if desired, automated download of significant Microsoft security updates. We have ongoing efforts to improve these services by ensuring that patch and antivirus servers are available in places with limited bandwidth, and by ensuring that patches are available from vendors, even though the Internet may be unavailable.

The Gold Disk is intended to help here as well. Updates of the Gold Disk are provided when new vulnerability information changes the standard DoD configuration. The Gold Disk is

then available, either via CD ROM or via download on all DoD networks, to help system administrators update previously configured computers.

Each of the capabilities described above is helping to make compliance actions easier and faster. However, Commands that own and manage significant numbers of computers can still have a tough time understanding whether each computer is configured properly, and whether patches mandated by IAVAs have been installed everywhere. DISA has several efforts to help administrators and Commands understand how well they are doing to comply with the standard configurations and updates mandated by IAVAs. In addition to the system auditing tools contained in the Gold Disk, each month DISA produces scanning scripts and configuration files for popular configuration scanning tools. These are available on all DoD networks and are intended to help a system or security administrator understand how well each machine conforms to the DoD standard configurations and whether all appropriate patches are applied. In addition to helping system administrators, these tools also help provide more accurate vulnerability management reporting and accountability. DISA also provides the DoD-wide means of reporting vulnerability remediation compliance.

Our major new technology initiative is the U.S. Strategic Command chartered effort to acquire DoD-wide licenses for commercial tools to help take inventory, and then detect and resolve vulnerabilities. Through the Information Assurance/Computer Network Defense Tools Steering Group, the Combatant Commanders, Services, and Defense Agencies have engaged to support consistency in implementation and use of these tools. This effort has now moved to the stages of a DISA-led acquisition, currently underway. This capability will build upon DISA's current program of providing scripts compatible with the vulnerability scanning tools already purchased and used throughout the Department. It will also provide a more comprehensive

deployment and more consistency in the application of remediation actions throughout the Department. We expect award of a DoD-enterprise scanning tool license this summer, with a remediation tool license in early fall.

As good as the supporting technologies, commercially available products, and implementing policies are, there are significant personnel components to this problem as well. Legacy environments; lack of vendor support for some still operational product lines; user and systems administrator training; and competing priorities for scarce resources require further focus. The DoD Certification and Accreditation process is just one step in providing this focus. Augmenting certification and accreditation and the regular use of vulnerability management tools, with a regular verification and support program, has helped to improve the DoD's security posture. DISA executes a robust verification program focusing on high-risk sites, such as the Combatant Commander networks and the classified networks. These programs, known as the System Readiness Reviews and Information Assurance Readiness Reviews are designed to look at the configuration and patch management programs within an organization; the overall security posture of their networks; their conformance with the STIGs and overall defense-in-depth principles; and are augmented with a traditional security review that considers continuity of operations, physical, and personnel security. DISA executes more than 120 of these reviews a year and has set standards for the military services to follow in order to expand the number of support visits, because more are necessary.

The Department as a whole has come a long way toward executing a meaningful vulnerability management program. There is still much work to do, not just in the sustaining base environment, but also in the highly dynamic operational commands where machines are continuously coming and going. Operations ENDURING FREEDOM and IRAQI FREEDOM

have driven home the challenges of operating information technology in the tactical environment, where access to commercial tools, to support, and to the time necessary to manage configurations are all very limited. We will continue to ensure that DoD and DISA efforts properly focus on the unique problems of our deployed warfighters.

Despite all of the good work, commercial product support, technology solutions, and leadership focus, nothing is fool proof. A configuration and patch management program must be implemented as a part of a robust and far-reaching Defense-In-Depth program. It is this program that enables the other work and serves to mitigate the remaining risks. Implementation of defense-in-depth includes: establishment of a secure DoD perimeter; maintenance of the security of the networks and transport infrastructure, including the routing and naming infrastructures; deployment of a secure, classified command and control network; and implementation of "demilitarized zones" for separating our internal Department computing from that of our partners, our allies, and the Internet. It is this secure environment, operated as part of overall DoD warfighting via NetOps, that is vital to DoD reliance on the GIG.

Mr. Chairman, members of the subcommittee, again, thank-you for the opportunity to appear before your subcommittee.

Mr. PUTNAM. Thank you. Is belly button a technical term or is that Defense jargon? [Laughter.]

Our next witness is Daniel Mehan, the Assistant Administrator, Information Services and Chief Information Officer, Federal Aviation Administration. In that capacity, he is the principal advisor to the Administrator on the agency's information technology and directs strategic planning for information technology across the agency. He oversees the implementation of the FAA's information system security, E-Government and process improvement programs.

Prior to joining the FAA, Mr. Mehan spent 30 years at AT&T where upon his retirement he served as international vice president for quality and process management.

Mr. Mehan graduated from Drexel University with a Bachelor's Degree in electrical engineering. He also has a Master's in systems engineering and a Ph.D. In operations Research from the University of Pennsylvania.

Welcome to the subcommittee. You are recognized.

Mr. MEHAN. Good afternoon, Mr. Chairman and members of the subcommittee. It is my pleasure to appear before you today to provide a perspective on the challenges of securing information systems in a Federal/civilian agency and to share with you the model the FAA has developed to address these challenges over the next several years.

I would like to commend the subcommittee for holding this hearing on the effects of our cyber security program and to acknowledge my colleague, Lisa Schlosser, the Department's Associate CIO for Information Technology Security.

The FAA maintains, operates and regulates the largest and most complex aviation system in the world. Effective management of a vast web of information about aircraft, weather, runway conditions, navigational aids and myriad of other elements is paramount to accomplishing our mission. To secure its cyber infrastructure, the FAA is implementing an android model for cyber defense depicting on the easel to your left that emulates one of the most resilient systems in the world, the human body. This holistic view enables the agency to address both short and long term cyber security objectives within the context of a unified framework.

There are six principal elements of the android cyber defense and they are analogous to six facets of the human body's defense. The three on the left side of the android are: architecture simplification, element hardening and boundary protection are the ones that have received the most attention historically and I would like to address them first.

Architecture simplification is analogous to nutrition and exercise. It is designed to ensure that the cyber infrastructure is in good shape to resist an attack. In this area, we are developing a technical reference model and common access architecture that will become the road map for effective information technology applications in the future. We are also ensuring that the number of systems in our inventory declines over time as we establish a more streamlined information technology architecture.

Element hardening is analogous to protecting major organs such as the heart and lungs. This element focuses on vulnerability management since it is about discovering vulnerabilities and setting

priorities to conduct remediation. The FAA will complete security certification and authorization packages on more than 95 percent of its systems by the end of this month. In addition, more than 1,600 FAA servers are scanned on a regular basis in order to identify and reduce the number of vulnerabilities per server. Results in these areas are included as key metrics in the FAA's overall management plan known as our flight plan which is reviewed monthly with Administrator Blakey.

With respect to patch management, the FAA has established policy and is currently using patch management tools to deliver software patches on our systems. We are also completing the requirements for a departmentwide patch management tool set which will allow for an enterprise-wide license and standardized approach.

Boundary protection is analogous to skin and membrane. It is the first line of defense against invaders. The FAA has significantly improved its boundary defense by reducing the number of authorized Internet access points, by implementing a new email system that reduces the number of mailboxes from 855 to 12 and by beginning to deploy the new FAA telecommunications infrastructure.

We believe there are tangible benefits being gained from our focus on the three left side elements of the android demonstrated by the fact that the agency and the Department have fared well in the recent cyber storms of Sasser, blaster and nimda. That said, there is much more to do.

The FAA is on a path to modernize its air traffic systems and to use more commercial, off the shelf products. The agency will also augment the three elements on the right side of the android model: orderly quarantine, systemic monitoring and informed recovery.

Orderly quarantine is analogous to the human body's immune system. We need a cyber immune system that can find, analyze and cure previously unknown viruses faster than the viruses can spread. Human intervention must be eliminated for portions of the defense because of the necessity to react quickly. Increased research will be required in the coming years to develop practical defense capabilities in this challenging area and it is an area where people process and technology must be blended.

Systemic monitoring is analogous to monitoring the vital signs of the body on a continuous basis. The FAA wants to implement an IT infrastructure that can detect failures in near real time and protect and heal itself. This capability requires the system to know its environment and to act accordingly. Self awareness and autonomic capabilities are still embryonic. One challenge in these operations is that input from a large number of network sensors involves enormous amounts of data that must be processed. The FAA has begun incorporating into its Computer Security Incident Response Center a data fusion capability using the next generation of tools to conduct data aggregation and event correlation to detect anomalous behavior.

Informed recovery is analogous to medical regimens such as administering antibiotics and undergoing surgery. Informed recovery and complex information systems is the set of actions that occur after there has been a cyber security incident. For the FAA these actions will include advisories from our CERT, establish procedures to be followed during an alert and orderly backup and recovery

mechanisms. Since a key requirement is to shrink response time, one of the near term goals is to converge vulnerability scanners, trouble ticketing programs and patch management software in order to automate more of the process from scanning to notification to remediation. The private sector can advance this initiative by exporting system message logs to an external bus so that this information can be used in real time with the other data sources.

To conclude, Mr. Chairman, the FAA, with the entire Department of Transportation, is complying fully with FISMA and has fared well using its multi-layered defense approach in the face of recent viruses and worms. That said, cyber defense over the balance of this decade must rely on the total android. The FAA will meet this challenge through a coordinated application of traditional and emerging techniques that provide a comprehensive approach to cyber defense. The android model presents a unifying framework for addressing cyber security on such a comprehensive basis.

To make one final human analogy, no one can guarantee we will never catch a cold but we need to be sure it doesn't become a case of pneumonia. The FAA and the Department of Transportation are dedicated to achieving that objective.

That concludes my remarks, Mr. Chairman. I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Mehan follows:]

STATEMENT OF DR. DANIEL J. MEHAN, ASSISTANT ADMINISTRATOR FOR INFORMATION SERVICES AND CHIEF INFORMATION OFFICER, FEDERAL AVIATION ADMINISTRATION, BEFORE THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM, ON INFORMATION SECURITY, JUNE 2, 2004

Good afternoon Chairman Putnam, Representative Miller, Members of the Subcommittee:

It is my pleasure to appear before you today to provide a perspective on the challenges of securing information systems in a federal civilian agency and to share with you the model the Federal Aviation Administration (FAA) has developed to address these challenges over the next several years. I would like to commend the Subcommittee for holding this hearing in order to highlight the important work that agencies must do to protect vital government systems. I would also like to emphasize that the FAA works collaboratively with the Department of Transportation (DOT) in all aspects of our Information Technology (IT) Security Program, and to acknowledge my colleague Lisa Schlosser, the DOT Associate CIO for Information Technology Security, who is with me at this hearing. In all of our activities, DOT and FAA work closely with other government initiatives. For example, we share incident information with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (CERT), and we have also worked with the National Science Foundation, the Air Force Research Lab and other government cyber security experts on a variety of research topics.

The FAA maintains, operates, and regulates the largest and most complex aviation system in the world. Effective management of this vast and complex web of information about aircraft, weather, runway conditions, maintenance facilities,

navigational aids, and a myriad of other elements is paramount to accomplishing our mission. This emphasis on information management brings with it a need to ensure that data is neither corrupted nor disrupted as it is shared across today's interconnected world. To secure its cyber infrastructure, the FAA has developed and is implementing an "*android*" model for cyber defense (see attached pictorial diagram) that emulates one of the most resilient systems in the world—the human body. This "holistic" view enables the agency to address both short-term and long-term cyber security objectives within the context of a unified framework.

There are six principal elements of the android cyber defense; and they are analogous to six facets of the human body's defense. The three on the left side of the *android*--architecture simplification, element hardening, and boundary protection—are the ones that have received the most attention historically, and I would like to address them first.

- Architecture simplification is analogous to nutrition and exercise. It is designed to ensure that the cyber infrastructure is in "good shape" to resist an attack. In this area, we are working on the development of a technical reference model, common access architecture, and desktop standards that will become the roadmap for effective information technology applications and services in the future. We are also ensuring that the number of systems in our inventory declines over time as we establish more streamlined information technology architecture.
- Element Hardening is analogous to protecting major organs, such as the heart and lungs. This element focuses specifically on ***vulnerability management*** since it is about discovering vulnerabilities, setting priorities to conduct remediation, and

applying appropriate resources for our critical systems. The FAA will complete security certification and authorization packages (SCAPs) on more than 95 percent of the systems in its inventory by the end of this month. Each SCAP has a plan of action and milestones that identify the most effective strategy to remediate vulnerabilities. In addition, more then 1600 FAA servers are scanned on a regular basis in order to identify and reduce the number of vulnerabilities per server. Both the SCAP completion targets and the vulnerability reduction targets are reviewed with the Department's Office of the CIO and are included as key metrics in the FAA's overall management plan, known as our *Flight Plan.* Our *Flight Plan,* which is reviewed monthly with Administrator Blakey, links the agency's activities through 2008 to our budget requests. It aligns all of our business plans, including information services, to ensure accountability at all levels.

With respect to patch management, the FAA has established policy and is currently using patch management tools to deliver software patches on our systems. In a broader context, we are working with the Department's Office of the CIO to complete the requirements for a DOT-wide patch management tool set. Such a tool set will allow for an enterprise-wide license and standardized approach to patch management for all DOT operating administrations, a significant contributor to securing the enterprise.

- Boundary protection is analogous to skin and membrane; it is the first line of defense against invaders. The FAA has significantly improved its boundary defense through three initiatives: first, reducing the number of authorized internet access points; second, implementing a new e-mail system and reducing the number of mailboxes

from 855 down to 12; and third, by beginning to deploy the FAA Telecommunications Infrastructure, a communications network that is fundamentally designed to provide a higher degree of computer security.

We believe there are tangible benefits being gained from our focus on these three left side elements of the *android*, most notably demonstrated by the fact that the agency and the Department have fared well in the recent cyber storms of Sasser, Blaster, and Nimda. That said, there is *much more to do*.

The FAA is on a path to modernize its air traffic systems and to use more commercial off-the-shelf products. With this significant emphasis on implementing air traffic control enhancements, the agency will also improve its layered protection scheme by augmenting the three elements on the right side of the *android* model: orderly quarantine, systemic monitoring, and informed recovery. These critical elements describe the "other side" of our cyber security concept:

- Orderly quarantine is analogous to the human body's immune system. We need a cyber immune system that can find, analyze, and cure previously unknown viruses faster than the viruses themselves can spread. Human intervention must be eliminated for portions of the defense because of the necessity to react very quickly. Increased research will be required in the coming years to develop practical defense capabilities in this challenging area. In addition, it will take considerable policy discussion, operational analysis, and system testing before those charged with protecting the an agency's network, the FAA's for example, will "turn over" the

quarantining of significant portions of it to an automated security system. So an enormous amount of research and development is required in this area in both the public and private sector, and it is an area where people, process and technology need to be blended.

- Systemic monitoring is analogous to monitoring the vital signs of the body on a continuous basis. The FAA wants to implement IT infrastructure and systems that can detect failures in real or near-real time and protect and heal themselves. This capability requires the system to know its environment and act accordingly. Self-awareness and autonomic capabilities are still largely embryonic. One challenge in these operations is that input from a large number of network sensors often exceeds millions of packets per day, potentially triggering thousands of alarms. The FAA has begun incorporating into its Computer Security Incident Response Center (CSIRC) into a data fusion center, using the next generation of tools to conduct data aggregation, data reduction, event correlation, and to detect anomalous behavior. Vendors are beginning to offer enterprise management consoles that attempt to provide "self-healing," but this is an area that needs to become much more mature in the near future. This model is also being piloted with DOT and the Department of Homeland Security to assist in creating near-real time information sharing that can ultimately be leveraged to protect the entire national infrastructure from the cyber threat.
- Informed recovery is analogous to medical regimens such as administering antibiotics and undergoing surgery. Informed recovery in complex information systems is the set of actions that occur after there has been a cyber security incident. For the FAA,

these actions will include advisories from our CSIRC and the Department's Transportation Cyber Incident Response Center (TCIRC), established procedures to be followed during an alert, and orderly backup and recovery mechanisms. Since a key requirement is to shrink response time, one of the near term goals is to converge vulnerability scanners, trouble-ticketing programs, and patch management software. The desired outcome is to automate more of the process from scanning to notification to remediation. The private sector can advance this initiative significantly by designing systems that export system message logs to an external bus in a standardized format, so that the information could be used in real time with the other data sources.

To conclude, Mr. Chairman, the FAA, with the entire Department of Transportation, is complying fully with the Federal Information Security Management Act (FISMA) and has fared well using its multi-layered defense approach in the face of recent viruses and worms. That said, cyber defense over the balance of this decade needs to rely on the total *android* and requires effort in areas where it is frankly more difficult to set up scorecards and audits. For the FAA, we will meet this challenge using a three pronged approach:

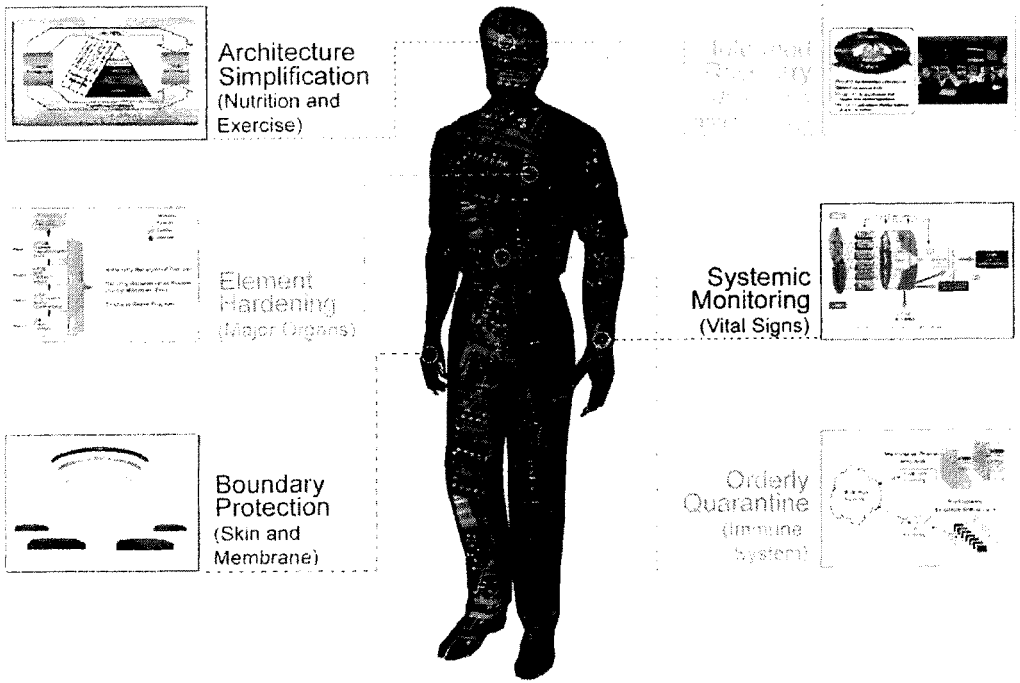
1. We will continue to implement "traditional" cyber activities around architecture simplification, element hardening, and boundary protection.
2. We will continue to help shape the nation's research agenda associated with orderly quarantine, systemic monitoring, and informed recovery. This requires

extensive interaction and partnering across a variety of educational, government, and private sector groups.

3. Finally, we will orchestrate a coordinated application of traditional and emerging cyber defense techniques to provide a comprehensive approach to cyber defense. The *android* model presents a unifying framework for addressing cyber security before, during, and after cyber attacks.

To make one final human analogy, no one can guarantee we'll never catch a cold, but we need to be sure it doesn't become a case of pneumonia. The FAA and Department of Transportation are dedicated to achieving that objective.

That concludes my remarks Mr. Chairman; I would be pleased to answer any questions you may have.



The "Android" Cyber Defense Model

Mr. PUTNAM. Thank you, Mr. Mehan.

Mr. Clay, would you like to make any opening statements?

Mr. CLAY. No, I will forego the opening statement and get right to the questioning.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
Computer Security

June 2, 2004

Thank you Mr. Chairman for holding today's hearing on network vulnerabilities and appropriate strategies that can be employed to counter the efforts of those seeking to damage information networks which the public and private sector depend on. As this subcommittee continues in its pursuit of appropriate solutions, I hope our witnesses can offer us new perspective on short and long-term strategies for strengthening our nation's computer security efforts.

According to the CERT Center at Carnegie-Mellon University, there were approximately 13,000 security vulnerabilities that resulted from software flaws beginning in 1995 through 2003. In addition, the number of computer security incidents reported to the CERT Center increased from roughly 10,000 in 1999 to over 137,000 in 2003. These numbers are alarming when considering our nation's growing dependence on information systems to conduct its daily affairs.

Although efforts have been made to combat network vulnerabilities, the constant change in technology and methods used by hackers make education a crucial component of addressing computer security goals and standards. We have little choice but to pursue these efforts, as a widespread and well-orchestrated cyber attack would be devastating to our nation in both economic terms and consumer confidence.

For the federal government, the sustained daily management of its computer networks is central to establishing adequate computer security standards. Although the use of patch management has proven to be an effective counter measure to exploits from external sources when systems are appropriately maintained, many public and private sector employees and vendors overlook such methods. If we are to avoid the severe problems experienced through episodes like the "Nimda" worm or the "Slammer" virus, managers must be educated on the latest patches and configuration management technologies available for their systems.

I want to thank our Chairman for his continued work and dedication to these issues. Mr. Chairman, this concludes my remarks, and I ask that they may be inserted into the record.

Mr. PUTNAM. Very well. I will recognize you for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman, for holding this hearing. I guess I had better start with Mr. Dacey.

I would be interested to know your views on whether FISMA ought to be reexamined to address issues of cyber security in the Federal Government? Are there specific issues that should be addressed in this Congress, in particular?

Mr. DACEY. In terms of FISMA, I think the law itself is fairly complete and comprehensive. I think there are a number of steps still underway, certainly the development of standards by NIST, the continuing refinement and development of some of the performance measures and reporting processes to assist the Congress in oversight. At this point, I don't have any specific changes that would be required but I do suggest that Congress should continue, and this subcommittee in particular, as it has, to monitor the progress of FISMA's implementation. There certainly have been challenges identified that need to be addressed and those need to go forward and continue to be monitored and improved over time.

Mr. CLAY. Based upon your survey, what patch management practices do agencies need to focus on?

Mr. DACEY. The areas that we looked at, and this is a survey and self reported information, but overall, we found there were some practices that were consistently applied. I think the area that was interesting to me personally was the number of agencies that did not have agencywide patch management policies and procedures. I think what I said before was a third said they didn't have agencywide policies and about 40 percent said they didn't have procedures. I think that is an important area because unless you have a consistent approach to patch management in the agency, there is a high likelihood that you are going to do it in an ad hoc manner and be consistent in protecting your infrastructure.

In terms of some of the other areas, I think in risk assessments in terms of testing and monitoring, I think all the respondents said they were doing some level. There were some agencies, however, that were kind of at the top end, testing all patches, doing formal risk assessments. I think there is some variation in the extent to which they are applying those practices and that might be something to continue to look at and determine whether or not some of those agencies should come up a level in terms of their adoption of those practices.

Mr. CLAY. Thank you for that answer.

Mr. Yoran, your testimony mentions efforts underway to develop a comprehensive operational partnership called the U.S. CERT Partner Program for Improved Security Response Efforts. Can you describe for us the key changes that you feel will demonstrate improvements over current U.S. CERT efforts? Is the private sector embracing these efforts or are there pockets of resistance within certain industries or sectors?

Mr. YORAN. There are a number of improvements between the partnership program which the U.S. CERT is undertaking and the existing paradigm. In many cases, the national response in cyber security has historically been coordinated by a number of private and trusted relationships and we will continue to encourage those relationships but at the same time, we recognize a need as our Na-

tion's dependence on technology increases, the need for us to institutionalize many of those interactions and institutionalize the response as a Nation to cyber activities and incidents. So the focus in the partnership program is to really extend the existing practices surrounding incident response, to institutionalize them, to promote the dialog and structured relationships that can promote a more effective response going forward.

In terms of reluctance or resistance to such a partnership program, we have been very encouraged by the enthusiasm of the private sector to interact with the Department of Homeland Security and in fact with the other departments and agencies in the Federal Government in a coordinated national response activity. So I think in large part, we are very pleased by the response.

Mr. CLAY. Let me ask, did you deploy any of the national cyber alert systems recently with the different viruses and worms and how did that work?

Mr. YORAN. We have issued a number of alerts. The National Cyber Alert System went live January 28, 2004. We have issued a number of alerts based on our analysis, based on feedback in collaboration we have had with other departments in the Federal Government and also with numerous entities in the private sector providing us their analysis and opinion on severity of vulnerabilities and the breadth of ongoing activities.

In terms of the effectiveness of that program, we have had in just a few months time over a quarter of a million direct subscribers, people looking for the types of information which we are publishing to them and we have also established relationships with other programs such as Infoguard and other entities which are actively engaged in responding to cyber security activities. They are also distributing that information. So we are pleased with the progress of that alert system and the private sector has also engaged us in numerous incidents where they want to leverage our capability to help get out the word about a particular vulnerability. A case of that might be where Cisco had a number of vulnerabilities a few weeks ago and they wanted to ensure that the word got out about those vulnerabilities to the folks responsible for protecting those routers. Through that relationship, we are able to help them in that effort.

Mr. CLAY. For Ms. Meyerriecks, how do you assess the risk associated with different vulnerabilities? Does this affect your approach in monitoring your networks for vulnerabilities and attacks? In one of your handouts, you talk about DOD employees using their personal home computers. How secure is that practice?

Ms. MEYERRIECKS. Let me make sure that I clarify that. Our employees use not their work computers but their personal computers at home and when they find something that is useful and many of us work long hours, I am sure you can relate, they may in fact bring in a disk or some other media. When we did the enterprise license for antivirus and associated things, we actually licensed it such that they could also use it for home use on their home computers.

Mr. CLAY. I wonder how much work they actually take home. I am just curious.

Ms. MEYERRIECKS. At least some of us work lots of hours which I am sure you can relate to. I just wanted to be clear on that.

The reason we categorize the threats is a risk assessment strategy that we take and if it is categorized as a relatively low threat, then we can react to that at a different pace than we would if something looked like it could cause a real compromise. That is intrinsically why we categorize things. The things I talked to today, the category I and II are those things we think would have most mission critical impact. We work those at a much higher priority, much higher pace. In lots of cases, we are actually supplying to other folks the code and sharing information very, very early on so that we are positioned to respond very quickly to the threats before they become widely known, publicly or can be exploited. That is part of our risk management mitigation strategy that we have categorized things to respond in that way.

Mr. CLAY. Thank the panel for their answers.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay.

Ms. Evans, in FISMA, there is a section that targets vulnerability reduction requiring each agency to develop specific system configuration requirements. Can you elaborate on the steps that have been taken or will be taken to enforce this provision?

Ms. EVANS. We have sent out our draft FISMA reporting guidance to the agencies for this year, fiscal year 2004. We are specifically asking questions about how they are putting together the configuration management and how they are managing that particular aspect of the act. As I said in my statement, we are asking specifically if they are using industry benchmarks, how they are managing the process and how they identify vulnerabilities. This is an ongoing process of which the IGs are also involved through verification of agency data and assessment of the process and look at how the agency, the department's management of the IT security program overall. We are specifically addressing the configuration management issue this year as well and asking the IGs to look at that.

Mr. PUTNAM. Part and parcel of that, how great an obstacle is it that so few agencies have completed the reliable inventory of assets? How does that play into vulnerability management?

Ms. EVANS. As we previously discussed during the March hearing, we agree that this really is the heart and soul of the issue and that it is difficult for an agency to say they have secured 90 percent of their systems if there isn't a good management process in place to identify the inventory of those systems. Again, in the fiscal year 2004 guidance, we are stressing that point and asking the IGs to look at how that process is being managed within the agency and whether inventory is being updated. We have taken your concerns very seriously and we too have asked those questions.

As you know in the scorecard one of the criteria that is in place in order for agencies to go green, they have to be able to show that they have certified and accredited 90 percent of their systems. The basic question we are asking is, how they identify the 90 percent, and how they can assert that this 90 percent is based off of the covered inventory and whether there is a good process in place to manage this invention before an agency will really move to green.

Mr. PUTNAM. Mr. Yoran, FISMA also requires each agency to establish minimum security configuration standards for the system they deploy. I would expect DHS is the leading agency in meeting this requirement so that other agencies can learn from your experience. What have you done to develop minimum security benchmarks?

Mr. YORAN. We are working actively with a number of organizations within the Federal Government to help establish those standards. Clearly it is not an effort which can be done within the Department of Homeland Security in isolation. To that end, we are working with NIST on those efforts and we are also working with the Center for Internet Security and making sure that the standards which are produced by the Center are readily available to those departments and agencies should they choose to adopt them for their own systems. It is also an area where we believe significant progress can be made working with vendors and encouraging them to take stewardship for their products in producing security configuration guidelines for those products, not only for the Federal departments and agencies but for use in the private sector as well.

Mr. PUTNAM. Is it that partnership or some other testing facility that you have established to ensure applications are not negatively infected by the more secure configurations?

Mr. YORAN. There are a number of testing labs and facilities both in the private sector and in the public sector to focus on vulnerabilities and configuration management. Our effort, specifically in the Control Systems Center of U.S. CERT and the test bed facility is to look at the control system and SCADA applications which are in use in the critical infrastructures and to increase emphasis, focus and testing of their security features and mechanisms.

Mr. PUTNAM. Section 3544 of FISMA describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." That same section also requires that each agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by the agency, another agency, contractor or other source." OMB's guidance in 2003 states, "Agencies are responsible for ensuring appropriate security controls for third party systems that have access to Government systems."

In my 2003 FISMA report card, the majority of agencies had not reviewed FISMA compliance with their contractors. What steps are being taken to remedy this and who is, to borrow Ms. Meyerriecks' term, who is the belly button to ensure this is happening? We will start with you, Ms. Meyerriecks.

Ms. MEYERRIECKS. Because of the sensitivity of the mission that the Department has, we have for many years put in place in our contract and acquisition strategy security criteria, particularly for developers and administrators of mission critical classified systems. That is has been a common practice for us for a number of years. I want to distinguish a couple different levels of contract support that we do. There are contractors that administer systems in our environment, on our behalf. They fall into the exact same set of cri-

teria that any of us do as a Government or military employee of the Department of Defense. It may be contractor maintained but it is a Government asset, so we apply the exact same physical security, information technology security. That is in our best interest and we have done that because of the criticality of the mission.

The second level I think is what you were poking at more directly and that is the people that supply products to us. Those folks, because of the acquisition strategy that we have in place, have to fall under the same sort of criteria. For example, if you are doing mission critical command and control for us, then there is a common security classification clearance required as well as for example, contractors cannot work in our building unless they have a secret level DOD clearance and have had that in place for quite some time.

If you are poking at the commercial industry, that is another step we would need to work with OMB and the rest of the agencies to look at what the implications are there. That is very far reaching as you are well aware.

Mr. PUTNAM. Ms. Evans.

Ms. EVANS. As part of our FISMA guidance, we do provide a question and answer section to clarify these types of issues going forward to the agencies. As far as asking who is responsible, the way that FISMA is set up, each agency head is responsible for the management of their overall security program. Therefore, if they make use of multiple contract services, the issue of how they manage their overall security profile needs to be addressed. We are planning to look at that this year along with the other issues that we have talked about, such as configuration management.

Mr. PUTNAM. Mr. Dacey, do you want to add anything to that?

Mr. DACEY. Just a couple comments. When we did the first GISRA implementation, identification was made that contractor systems were a problem because a lot of agencies weren't considering them. In last year's FISMA reporting we got a bit of improvement but there was a discrepancy to some extent in this particular measure between the IGs and the CIOs reporting the information. The CIOs said as my records indicate 22 agencies said they did manage and monitor their contractor systems appropriately. The IGs said about half of them did. So there was some difference. I think that is one area as we talked about in March that further refinement of the type of information we are getting back would be very helpful. Right now there is basically one question that says are you monitoring and supervising your contractor systems. I think if we were to look at that and perhaps gain a bit more information in the next reporting cycle, which Ms. Evans alluded to, I haven't seen what you are asking for, that could help get that information. I think that is an important area.

I still think there are areas that haven't been explored and OMB's guidance talks about State and local governments. The Federal Government has lots of systems that interact with State and local systems particularly in the benefits area. That is an area that I don't know has been explored a lot. I know in some areas there has been a lot of exploration. Medicare contractors have long been supported. I know DOD has done that for several years. So I think that is an area where we need to keep looking closely. I think that

is a risk area as evidence from our control system testimony. A virus gotten from a contractor system right into the Davis Bessey nuclear powerplant which fortunately at that time was under maintenance but it just goes to show there are lots of avenues and opportunities. We routinely test some of those areas when we do our security reviews, particularly where contractors are regularly into agency systems.

Mr. PUTNAM. Mr. Mehan, you mentioned your agency's total compliance with FISMA. Does that include the OMB's guidance regarding third party systems and contractors?

Mr. MEHAN. Yes. We have put a lot of focus on personnel security. Our contracts have all been modified to be sure that wherever people are dealing with information technology and have access to our systems, the appropriate clearances are provided and that we know the people who are using those systems.

I will tell you though that just as in the long run, there are more sophisticated techniques that will be used, it is our intent over the longer run to eventually use biometrics to test the entry of contractors or others to our systems on a more controlled and daily basis.

Mr. PUTNAM. Mr. Dacey, as I mentioned in my opening statement, my concern is not only on how future systems will be protected but how we retrofit current systems and improve their security and integrity, cleaning them, protecting them and making sure they are not immediately spreading something to the newer systems. Some suggest that Federal systems have already been compromised and are currently being used as attack tools. What are your thoughts on that? Obviously it is very alarming and how do we go about identifying those and cleaning up those systems?

Mr. DACEY. There are a couple of issues there. One is the challenge in the Federal environment particularly of applying patches and other techniques to protect those systems in the first place. Again, prevention is the first step. I think the challenge there is how do we keep the system patched. We have control systems with unique characteristics that you can't just apply a patch, it might break your control system and the vendors sometimes take a while to understand and assess the patches before they can apply them because those control systems rely upon some of the same operating systems that vulnerabilities occur.

Additionally, in applying patches, testing them is a major challenge. I think if you look at successful agencies or private sector actually, and I think you made some visits in the field, you will see they have standard builds. We talked about it here at DISA, we are hearing about that at Agriculture and other places. If you don't have standard configurations, you don't know how your systems are going to react when you start applying these patches and making the fixes. So I think that is another area we need to keep looking to in terms of that, and a very critical area because it takes a lot of time if you have all disparate systems to understand how these patches are going to affect them.

The third area is just looking at some of these other practices we talked about today, defense in-depth and some of the other strategies, not just patching but how do we protect the whole by providing layers of protection. Related to that as part of FISMA is the whole process of monitoring these systems, making sure we are

able to detect anomalous activities so if we do find someone is in there doing inappropriate things and stop it as quickly as possible. I can't speak to the extent to which that may be happening but certainly there have been reported instances where Federal systems have been attacked and used as servers for chat rooms, certainly some State systems have been used to do other activities because someone broke in and set up back doors. It does happen. I just don't know or have any information on the frequency but it is possible.

Mr. PUTNAM. Mr. Yoran, how effectively are we using other information technology management options, the Federal enterprise architecture comes to mind, to promote or ensure information security within the Federal Government? I will let you take first crack and then Ms. Evans.

Mr. YORAN. I believe we are leveraging the enterprise architecture. It is really an area that falls outside of the specific purview of the Cyber Security Division and I would defer to Ms. Evans.

Ms. EVANS. Thank you for asking that question. Actually, as we have discussed previously, the Architecture Committee of the CIO Council has been working on a security profile to overlay through all the models of the Federal enterprise architecture. The reason for this is to be sure that security is thought of through all aspects of the system life cycle as investments go forward. The Federal enterprise architecture, from our standpoint, is very critical and security needs to be highlighted from the very beginning of the planning of an investment all the way through the operations and maintenance of that investment. We have to ensure that we are leveraging best practices and components that have been deployed in other parts of the Government and the architecture will give us the tool with which we can do that. Several of the mechanisms and practices we are talking about will be brought to life as we leverage this profile. The Council is getting ready to release a draft of this profile to the CIOs for comment very shortly.

Mr. PUTNAM. Ms. Meyerriecks, take a moment if you would and give us some detail as to what security procedures DOD has implemented.

Ms. MEYERRIECKS. We could go on at length about those but some of the ones I think have been most effective, some of the things we have done in the past 12 months are the tightening up I spoke to in my testimony about the interfaces between the corporate intranet, our NPRA Net as we refer to it and the Internet in terms of the gateways but we were also in a situation several years ago and brought to the attention of the Secretary where we actually had no DMZ, a demilitarized zone, actually a common IT term as well but it fits the military very well in terms of where we put our public facing Web servers and portals. People were actually coming into our corporate intranet to hit those. That was a major issue because it made us very vulnerable to anybody who could exploit one of those in terms of getting into the corporation. So one of the major initiatives we took on in the last 12 to 18 months was to establish a demilitarized zone and put out practices and procedures for how a provider, and we have literally tens of agencies that provide public facing, consumer interfaces, how they could intersect with our demilitarized zone. It was actually funded as op-

posed to a fee for service initiative. Their responsibility is to put the servers in the zone and configure them properly so that they are not able to be used as a departure point for further exploit into the infrastructure. You see in our flattening curve actions like that have actually we think started to pay off in terms of penetration, successful penetration into our infrastructure.

Another very successful effort was also the STGS and the work we have done with NSA which is one of our sister agencies and also NIST, just a DOD/IC intelligence community, in terms of specifying secure configurations and the really good response we have had from all of our commercial providers in terms of being willing to learn from those and in some cases embrace those and ship product based on those configuration management guides.

I would say those are two things that have been force multipliers in terms of our ability to combat the threat.

Mr. PUTNAM. Do you have an agencywide patch management system?

Ms. MEYERRIECKS. We have a DOD-wide patch management system. DISA administers to a large extent that capability for the Department but it is very much a partnership with particularly the services in terms of distribution and command and control of how we distribute those patches. As my colleagues alluded, we do have unique applications, so there are places where an Air Force has a specific mission that might be impacted in a negative way by a particular patch because the vendors can't understand every implication. We roll them out at an enterprise level and then we do testing for each of the specific platforms where we have those sorts of applications to ensure that it is not going to have a dilatory effect on the actual application we are trying to support.

Mr. PUTNAM. Having laid out some of these strengths, maybe you can share why DOD's FISMA score is so bad.

Ms. MEYERRIECKS. We will have to take that for the record, sir. I don't have the background to address that. I apologize.

Mr. PUTNAM. We will let you answer that for the record.

Mr. Yoran, we spend $60 billion a year in IT hardware, software, annual investment by the Federal Government. Obviously DHS being something of a startup I merging all the disparate departments and agencies, you are spending a fortune and you have unique security requirements. How have you used the procurement power behind the needs that you have to really ensure that the security is baked in?

Mr. YORAN. That question really needs to be answered with a number of tier responses. Within the Department of Homeland Security, we are working with Steve Cooper's organization and the CIO shop to identify the security requirements of the Department and ensure that we are procuring those technologies which can address the security requirements which the CIO's office is ultimately responsible for identifying.

We also hope to be able to better leverage those requirements and in our interaction with the other departments and agencies of the Federal Government to work with the vendor community so that they can take some of those practices and improve the products which they are delivering to the Federal Government as a customer and to the extent that we can create consistency between our

requirements and the requirements of other critical infrastructure operators, BITS and the financial services, the American Chemical Council and the chemistry sector, and we can define these uniform requirements for the vendor community. I believe that will make their job a lot easier and a lot more focused in bringing us solutions which address these common requirements.

Mr. PUTNAM. Ms. Evans, do you wish to add anything to his comments on ways to leverage our $60 billion annual investment in high quality, more secure products?

Ms. EVANS. We do intend at OMB to use the Smart Buy initiative to really work on leveraging these security benchmarks. It will require partnership between the Government and industry but, I do believe, based on my past experience as the Department of Energy CIO, industry wants this partnership just as much as Government does. There is value to both parties coming together. The Government can make their expectations very clear. Industry benefits because the country as a whole will benefit from more secure products.

I think industry wants a partnership. I know we have talked to industry about that. We intend to leverage that same type of model that we used at Energy through the Oracle contract. That took a long time with the Center of Internet Security working on the benchmarks across several industry partners that were involved in coming up with those benchmarks. This work could be leveraged and can be used in the long run by everyone. It is our intention to do that. That is why we are asking about benchmarking, and as we continue to evolve the Smart Buy initiative we can take it to industry and say this is how we would like to proceed with our buying.

Mr. PUTNAM. Ms. Meyerriecks, do you wish to add anything? Obviously this is a huge concern for the Department of Defense software assurance. Do you have any comments on that?

Ms. MEYERRIECKS. I would just like to echo my colleague's statements regarding industry.

The other comment that I would make is one of the things that has also proven beneficial to us is efforts like the common criteria where we actually encourage vendors to think about how to make more secure products while they are still in the labs as opposed to negotiating a configuration after it has already been cut into the silicon if you will. Amit talked about the importance of influencing products earlier in their development cycle, so they are thinking about that as opposed to patching them afterwards. Common criteria has been especially useful. We ought to think about how we encourage more of that behavior.

Mr. PUTNAM. Mr. Mehan.

Mr. MEHAN. The only thing I would add to what my colleagues have said which I support is what vendors have told us is that it is important that in our request for quotes and so forth that we have the same enthusiasm for cyber security as we have in other rhetoric. The cyber security aspect of it was absolutely fundamental. In fact, vendors pretty much had to prove they could satisfy that before we got into too much else they were going to provide. That sent a strong signal to industry.

Mr. PUTNAM. This is a particularly good panel in terms of the agencies and departments represented for this topic. I really appreciate your participating. When you look at FAA and certainly the events that have transformed our approach to air travel and peoples' approach to security and safety, obviously the Department of Defense and certainly Homeland Security and all of you are in key positions to be crying in the night about the need for more emphasis on cyber security. Do the three of you have the ear, the access, the entre to your respective department or agency heads and do you believe that the cyber threat is being adequately addressed? Begin with Mr. Mehan and end with Mr. Yoran and then unfortunately we are going to have to bring this panel to a close. Mr. Mehan.

Mr. MEHAN. I clearly have access to the Administrator of our agency whom I report to directly. I also have access to the Department of Transportation CIO who is also the vice chair of the Federal CIO Council and we have the ear of the Secretary of Transportation. There is no lack of access to the top deck of Transportation and Aviation. I think it is a message that all of us in concert with Congress have to keep putting out to the public and putting out to the industry because I think one of our big challenges is in the second half of this decade, there is the potential that we could see more orchestrated, more sophisticated attacks and we have much to do in order to be ready for them. That is part of why we have laid out a long term model for approaching this.

Mr. PUTNAM. Thank you, Mr. Mehan. While we give Ms. Meyerriecks another moment to think through her comments, your android approach, your design, your idea, is very effective and we certainly appreciate the work that you are doing at FAA.

Ms. Meyerriecks.

Ms. MEYERRIECKS. I have my direct report to my agency head as well and we absolutely have access to our CIO who has made it one of their top priorities—it would be good to have one who wasn't an acting one if I could put in that plug—as well as access to the Secretary and this is a high priority for us. I share the concern that we not lose focus in terms of keeping it a high priority topic because with all of the demands on the resources of the Department we need to make sure that it stays front and center in terms of our leadership's interest and commitment to it, but it is not an issue today.

Mr. PUTNAM. Mr. Yoran.

Mr. YORAN. The Department of Homeland Security, I personally have spoken with Secretary Ridge, with Executive Secretary Lowey on cyber security issues and am confident in their focus and attention to cyber security as a very valid concern for our Nation. On a regular and ongoing basis, I have discussions about cyber security with the Under Secretary for Information Analysis and Infrastructure Protection, Under Secretary LaBudy and Assistant Secretary Laskowski.

Our approach is to continue to focus on an outcome based, integrated risk management approach which includes an active interest in cyber security as a vulnerability to our Nation.

Mr. PUTNAM. Thank you.

Mr. Dacey or Ms. Evans, do you have any final remarks before we dismiss panel I and seat panel II? Mr. Dacey.

Mr. DACEY. Just a brief comment. We have talked a lot about trying to address some of the security issues of the software as it is developed but I do think and FISMA promotes a consistent process to try to develop the standard minimum security guidelines by risk level as well as NIST is developing checklists which are consistent with the standard guidelines in the STGs that were talked about earlier. I think that is an important area because we need to continue to leverage that being done centrally because I don't think we can rely continually on the system admins to individually come up with the right solutions or even subcomponents of agencies. To the extent we can build in some clear processes, communicate those, develop training and so forth, that will go a long way because just with patch management if you are looking at maybe having 24 or 48 hours to get something fixed, that is not a long time. You have to look for more long range solutions to the problem.

Mr. PUTNAM. Ms. Evans.

Ms. EVANS. First, I would like to thank you again for having this hearing on cyber security. This is an important priority to the administration. We are taking steps to ensure that it does stay on the forefront as my colleagues have mentioned. We are doing this through the implementation of FISMA but as well as through the President's management agenda. Because this is a priority, we are trying to ensure that the agencies have the resources that they need in order to ensure they have good management practices in place to achieve the results of a safer infrastructure, and safer cyber security environment, so that we can move forward and use technology in a way that minimizes risk to us. Thank you again for the hearing.

Mr. PUTNAM. Thank you. Noting that there are no further questions, we will stand in recess while we reset the witness table for panel II. The subcommittee is recessed and will reconvene in just a few moments.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene.

I would ask the witnesses to take their seats, please.

[Witnesses sworn.]

Mr. PUTNAM. We will move immediately to testimony with Ms. Dubhe Beinhorn, vice president of Juniper Federal Systems and is responsible for the development and execution of all aspects of Federal engagements. Prior to joining Juniper in 2001, she was with SafeNet where she was general manager of the PKI hardware and software division and held responsibility for all aspects of this division including sales, systems, marketing, supporting and manufacturing. She has more than 25 years of experience in the Federal Government and the enterprise competing industry in both domestic and global markets.

Ms. Beinhorn holds a Bachelor's Degree in business from Roanoke College in Virginia. Welcome to the subcommittee. You are recognized for 5 minutes and I would ask all of our witnesses to please limit your testimony to 5 minutes as we have a large panel.

You are recognized.

STATEMENTS OF DUBHE BEINHORN, VICE PRESIDENT, JUNIPER FEDERAL SYSTEMS; SCOTT CULP, SENIOR SECURITY STRATEGIST, MICROSOFT CORP.; LOUIS ROSENTHAL, EXECUTIVE VICE PRESIDENT, ABN AMRO SERVICES CO., INC.; MARC MAIFFRET, CHIEF HACKING OFFICER, eEYE DIGITAL SECURITY; AND STEVE SOLOMON, CHIEF EXECUTIVE OFFICER, CITADEL SECURITY SOFTWARE, INC.

Ms. BEINHORN. Thank you, Mr. Chairman and members of the subcommittee. It is a pleasure to appear before you today to discuss the growing challenge of vulnerability management in information technology systems. You and the subcommittee have been leaders in raising awareness of the importance of network security in the public and private sectors. Your work with the Corporate Information Security Working Group is an important example of your commitment to ensuring a true public/private partnership for solving the very difficult challenge of cyber security.

At Juniper Networks we take our participation extremely seriously as we do our commitment to you, Mr. Chairman, in fully supporting active participation by CEOs, working groups and other forums all with an end goal of joint solution determination.

The challenge itself, the threats to today's networks continues to grow. Attacks continue to evolve and move from the network to the application level. They are more sophisticated, using new origination points and come from known and unknown sources. The problem is made worse because of the inability of much of the existing Internet infrastructure to identify and then block threats that emerge. More vulnerabilities are discovered every day. The time from discovery to exploit continues to shrink and the pressure placed on network administrators to remediate these vulnerabilities in a timely fashion continues to grow much like baling water out of a boat that continues to spring leaks. Patch management is only a short term fix and does nothing to solve the root cause of network insecurity.

Part of the challenge is the simple fact that the Internet is not just one network. It is multiple networks connected together. As such, it was never designed with security in mind. Its greatest strength, widespread connectivity at low cost, is also one of the greatest weaknesses. With low cost comes diminished value, unreliability and lack of security. Each network has its own security policy and as we all know, network security is only as strong as the weakest link.

At the moment, only isolated networks can guarantee infrastructure and data security from outside attacks. However, isolated networks work against netcentric enterprise services. Additionally, isolated networks do not address the problem of insider attacks and are cost prohibitive for many Government and enterprise networks.

Most people are focused on securing the enterprise. There is, however, another critical element. It is securing the fabric of cyberspace beyond the enterprise firewall, the space between the enterprises. President Bush, in his national strategy to secure cyber space, called for "securing the mechanisms of the Internet."

Right now, all packets travel over the same public network with the same priority and the same security. Part of the challenge is recognition that all packets are not created equal and we must de-

vise a security approach that assigns the right level of security for each packet that flows from its originator through the public network to its destination. This is the challenge.

First and foremost, service providers and networking companies of both private and public infrastructure play a critical role in alleviating the problem. All companies should be encouraged by Congress and congressional leaders to share information. Specifically, public and private industry forums should focus on pre- and post-attack vulnerabilities as well as real time attack isolation and prevention. All Internet stakeholders need to develop a set of industry best practices based on the information communicated by all forums. As an example, such collaboration may yield mechanisms to prevent users masquerading as other users and denying access in the first place, techniques for securing the network control plane so that false routes may not be hijacked or injected, thus preventing man in the middle attacks. Finally, the use of automated tools to conduct assessments and ongoing security audits to help identify vulnerabilities on the network and usual activity.

These tools can also be part of a larger effort aimed at creating a culture within companies as well as Government agencies of security awareness and responsibility. These industry best practices allow for malicious traffic to be identified, blocked and prevented from spreading. They give us the ability to quickly identify and quarantine hot spots and reduce the spread of viruses and the rising cost of businesses and consumers from such attacks.

The public network cannot stand alone in the protection of businesses, institutions and citizens. Security must also be established at multiple levels including application device and department levels. These security measures must be able to communicate with each other and with the network to form a level of protection that is greater than the sum of the parts. Networks must intelligently interact with the user and the application so that the level of trust can be established at the beginning of each network transaction.

Much work has been done by companies participating in the Web services movement and standards development effort. Local and wide area networks must leverage this work to extend the concept of trust agents and user federations to the network itself. The work is already underway. At Juniper Networks, along with 18 other industry leaders, we are working to build these standards to create networks that can deliver a specified level of security, performance and reliability. The group calls itself the Infranet Industry Council. It seeks to put existing technology and standards to work building on them when necessary to form an underlying communications infrastructure that provides the best attributes of public and private networks.

An infranet is a selectively open network with assured performance and security of a private network enabling a packet infrastructure to support all communications. Infranets can be built and operated by service providers, agencies and businesses and can be securely interconnected with each other for the purpose of giving users and on demand appropriately tuned to their unique security and quality requirements. At the appropriate time, we would welcome the opportunity to explain this further.

Over the long term, vulnerability management must be addressed by all Internet community members to design more secure systems and networks with a zero trust tolerance. This means there should be absolute distrust of outsiders and insiders. We should recognize both as equal threats and not give greater weight to one or the other. Building networks that trust no one is a far better approach to managing the threats and will ensure a higher level of security.

Juniper Networks' approach to network security is based on ensuring reliability, security and quality throughout the network. This commitment and our activities with public infrastructure providers and with the defense and intelligence community enables us to do our part to better secure our critical networks and play an active role as a member in the cyber security industry alliance.

In today's world, it is no longer about competing. It is about collaborating. With your help, Mr. Chairman, the Government initiatives to guide industry, vendors and all stakeholders will succeed in true joint development of a worldwide Internet capable of meeting its mission regardless of malicious intent, unforeseen failure or misadventure.

On behalf of Juniper, we thank you for the opportunity to be here today.

[The prepared statement of Ms. Beinhorn follows:]

Statement by Ms. Dubhe Beinhorn
Vice President, Juniper Federal Systems
Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
June 2, 2004

Mr. Chairman, Members of the Subcommittee, it is my pleasure to appear before you today to discuss the growing challenge of vulnerability management in information technology systems. You and the Subcommittee have been leaders in raising awareness of the importance of network security in the public and private sector. Your work with the Corporate Information Security Working Group is an important example of your commitment to ensuring a true public-private partnership for solving the very difficult challenge of cybersecurity. At Juniper Networks we take our participation extremely seriously as we do our commitment to you Mr. Chairman in fully supporting active participation by CEO's, working groups and other forums all with an end goal of joint solution determination.

The Challenge

The threats to today's networks continue to grow. Attacks continue to evolve and move from the network to the application level. They are more sophisticated, using new origination points, and come from known and unknown sources. The problem is made worse because of the inability of much of the existing internet infrastructure to identify and then block threats that emerge.

More vulnerabilities are discovered every day, the time from discovery to exploit continues to shrink, and the pressure placed on network administrators to remediate these

vulnerabilities in a timely fashion continue to grow. Much like bailing water out of a boat that continues to spring leaks, patch management is only a short term fix and does nothing to solve the root cause of network insecurity.

Part of the challenge is the simple fact that the internet is not just one network; it is multiple networks connected together. As such, it was never designed with security in mind. Its greatest strength – widespread connectivity as low cost – is also one of its greatest weaknesses. With low cost comes diminished value, unreliability and a lack of security. Each network has its own security policy and, as we all know, network security is only as strong as the weakest link. At the moment only isolated networks can guarantee infrastructure and data security from outside attacks. However isolated networks work against net-centric Enterprise Services. Additionally, isolated networks do not address the problem of insider attacks and are cost-prohibitive for many government and enterprise networks.

Most people are focused on securing the enterprise. There is, however, another critical element, securing the fabric of cyberspace beyond the enterprise firewalls, the space between the enterprises. President Bush in his National Strategy to Secure Cyberspace called for "securing the mechanisms of the internet." Right now all packets travel over the same public internet, with the same priority and the same security. So, part of the challenge is recognition that "all packets are not created equal" and we must devise a security approach that assigns the right level of security for each packet that flows from its originator through the public network and to its destination. This is the challenge.

The Near Term Response - Strategies

First and foremost, Service providers and networking companies (of both private and public infrastructure) play a critical role in alleviating the problem. All companies should be encouraged by congressional leaders to share information. Specifically, public and private industry forums should focus on pre and post attack vulnerabilities as well as real time attack isolation and prevention. All internet stakeholders need to develop a set of industry best practices based on the information communicated by all forums. As an example such collaboration may yield mechanisms, to prevent users masquerading as other users and denying access in the first place. Techniques for securing the network control plane so that false routes may not be hijacked or injected thus preventing man in the middle attacks. And finally use of automated tools to conduct assessments and on-going security audits to help identify vulnerabilities on the network and unusual activity. These tools can also be part of a larger effort aimed at creating a culture within companies as well as government agencies of security awareness and responsibility. These industry best practices allow for malicious traffic to be identified, blocked and prevented from spreading. They give us the ability to quickly identify and "quarantine" hot spots and reduce the spread of viruses and the rising cost to businesses and consumers from such attacks.

The public network, cannot stand alone in the protection of businesses, institutions and citizens, security must also be established at multiple levels including application , device, the department levels. And these security measures must be able to communicate with each other, and with the network, to form a level of protection that is greater than the sum of its parts.

Networks must intelligently interact with the user and the application so that the level of trust can be established at the beginning of each network transaction. Much work has been done by companies participating in the Web Services movement and standards development effort. Local and wide area networks must leverage this work to extend the concept of trust agents and user federations to the network itself.

The work is underway, Juniper Networks and 18 other industry leaders are working together to build on these standards to create networks that can deliver a specified level of security, performance and reliability. The group calls itself the Infranet Industry Council. It seeks to put existing technologies and standards to work, building on them when necessary, to form an underlying communications infrastructure that provides the best attributes of public and private networks. An Infranet is a *selectively-open* network that combines the reach and positive economics of the public network with the assured performance and security of a private network, enabling a packet infrastructure to support all communications. Infranets can be built and operated by service providers, agencies and businesses....and can be securely interconnected with each other.....for the purpose of giving users an on-demand network appropriately tuned to their unique security and quality requirements. At the appropriate time we would welcome the opportunity to explain this initiative further.

Over the longer term, vulnerability management must be addressed by all internet community members to design more secure systems and networks with a "zero trust tolerance" approach. What that means is there should be absolute distrust of outsiders

and insiders. We should recognize both as equal threats and not give greater weight to one over the other. Building networks that trust no one is a far better approach to managing the threats and will ensure a higher level of security.

Conclusion

Mr. Chairman, Juniper Network's approach to network security is based on ensuring reliability, security and quality throughout a network. This commitment and our activities with public infrastructure providers, with the defense and intelligence community, enables us to do our part to better secure our critical networks and play an active role as a member in the Cyber Security Industry Alliance. In today's world it is no longer about competing it's about collaborating. With your help Mr. Chairman, the government initiatives to guide industry, vendors and all stakeholders will succeed in true joint development of a worldwide internet capable of meeting its mission regardless of malicious intent, unforeseen failure or mis-adventure. On behalf of Juniper Networks and our CEO, Scott Kriens, thank you for the opportunity to speak before you today. I look forward to answering your questions.

Mr. PUTNAM. Thank you.

Our next witness is Scott Culp, senior security strategist for Microsoft Corp. As member of the Trustworthy Computing Team, Mr. Culp focuses on developing companywide security policies and procedures, evaluating the security of current Microsoft products and services and reaching out to the critical infrastructure protection community.

Mr. Culp is the founder and former manager of the Microsoft Security Response Center where he helped develop and implement leading security response capabilities.

Welcome to the subcommittee. You are recognized for 5 minutes.

Mr. CULP. Thank you for the opportunity to appear today. My name is Scott Culp and I am a senior security strategist at Microsoft. Delivering on the trustworthy initiative is one of Microsoft's top priorities and improving the manageability of security patches is an important part of that work.

A troubling recent security trend has been the dramatic shortening of the time between the issuance of a patch that fixes a vulnerability and the appearance of a worm exploiting it. In just the past several years, this window has narrowed from hundreds of days in the case of nimda to 26 days to blaster, to 17 days for the recent Sasser worm. In the face of this trend, Microsoft is employing a defense in-depth strategy.

First and foremost, Microsoft recognizes that the most effective improvement we can make with regard to patches is to require fewer of them and we are making substantial progress in reducing security vulnerabilities in our software but no software will ever be completely free of vulnerabilities and so we are improving entire patch management ecosystems. Over just the past year, we have largely standardized the operation of our patches, significantly reduced their size and reduced the need to reboot the system after applying them. In the next service packs for Windows XP and Windows Server 2003, we will deliver new technologies that will help protect systems even if the user has not installed all needed patches. In the longer term, we are developing break through technologies that will enable systems to dynamically change their behavior when needed patches are missing and to automatically recognize and defend against attacks.

At the same time, we are working to help raise Federal agency awareness of products and resources that address the requirements of the Federal Information Security Management Act and we are providing improved training opportunities for all our customers, including continuing our twice yearly Federal security summits. We are also contributing to important security policy initiatives. Within just the past few months, Microsoft co-chaired a National Cyber Security Partnership Task Force that recommended important improvements in the entire software development life cycle including patch management. We are working with BITS to address the financial sector's legacy and other needs and challenges.

These efforts and others underlie what we believe is the industry's leading incident response process. To highlight this, let me use the Sasser worm as an example. On April 13, 2004, Microsoft published a security bulletin and patch addressing the vulnerability that Sasser ultimately exploited. Microsoft's engineering

and educational efforts over the preceding months contributed to a patch uptake rate that was 300 percent higher than for last summer's blaster patch. We provided information, guidance and recovery tools for our customers worldwide, including contacting U.S. CERT at the time of the release of the bulletin and again when Sasser was discovered. Our antivirus reward program caused an individual to provide information to law enforcement that contributed to the arrest of the worm's alleged author.

Ultimately, we believe these actions reduced the worm's impact but the fact that it occurred at all reminds us that we need to continue improving. We all have roles to play in improving cyber security. As the Congress and the administration addressed this topic, we suggest several actions which we are eager to work with the Government on.

First, we hope the Senate will ratify the Council of Europe Cyber Crime Treaty. Second, our law enforcers are doing great work but need more training and better equipment. Third, Government systems administrators would benefit from more intensive training in security. Fourth, we support the common criteria process but believe it could be improved to make it more efficient and cost effective. Finally, we support increased basic research in cyber security and computer forensics.

In the final analysis, a more secure computing environment is best achieved when industry leaders continue to innovate around security to continuously improve the security of software products, help customers operate their networks more securely and to provide effective security and incident response processes.

I would like to thank the committee for this opportunity and I look forward to your questions.

[The prepared statement of Mr. Culp follows:]

Statement of Scott Culp

Senior Security Strategist, Trustworthy Computing Team
Microsoft Corporation

Testimony Before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
House Committee on Government Reform
U.S. House of Representatives

Hearing on "Cybersecurity and Vulnerability Management"

June 2, 2004

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee: My name is Scott Culp, and I am a Senior Security Strategist for Microsoft. Thank you for the opportunity to appear today. I would like to discuss patch management tools and processes that we have deployed and are continuing to improve, as well as the ongoing support we are providing and the innovation-driven technology solutions we are developing to help the federal government and all of our customers enhance the security of their computing environments. I am a member of Microsoft's Trustworthy Computing Security Strategies Team; its mission is to deliver on the security portion of Microsoft's Trustworthy Computing initiative. This is one of our company's top priorities, and I am focused on, among other topics, leading a corporate-wide initiative to improve patch management. Before joining the Trustworthy Computing Security Strategies team, I helped establish and, until 2003, managed the Microsoft Security Response Center, where I coordinated Microsoft's patch management and incident response programs.

As this subcommittee is aware, cybercrime is an industry-wide challenge, and we have developed sophisticated mechanisms designed to identify and mitigate software vulnerabilities before criminal hackers are able to exploit them. These steps, which include effective and rapid development, delivery, and installation of updates, are essential, but are not enough by themselves. One of the key security trends over the past three years has been the dramatic shortening of the time between issuance of a patch that fixes a vulnerability and the appearance of a worm carrying exploit code targeting that vulnerability. For the NIMDA virus, that period was 331 days. Only two years later, the Blaster worm shortened the window to just 26 days. And with the Sasser worm outbreak,

which was first identified on April 30, 2004, a mere 17 days passed between patch and worm.

As a result of this narrowing window, effective patch management, while essential, is not sufficient. We as an industry are innovating to develop and deliver new defenses designed to improve the security of users' systems. And for users who for one reason or another cannot apply patches to their systems, these other defenses are even more vital means to protect their systems. To help meet this need, Microsoft is employing a defense-in-depth strategy that goes beyond patch management to include advanced and security-focused software engineering, industry and government collaboration, and public education. My testimony today will focus both on patch management improvements we and our customers have made, and on how Microsoft's defense-in-depth approach can help to secure federal agencies' computing environments.

I. Microsoft's Patch Management Strategies

Microsoft recognizes that the most effective patch management strategy is to require fewer patches. We are making substantial progress in reducing the incidence of security vulnerabilities in our software. Nevertheless, the process of designing, writing and producing software is intensely complex, and software will never be completely free of vulnerabilities. So, even as we improve our software, we recognize that we must also continue to improve the quality of our updates, and the tools and processes that will help customers use them most effectively.

A. Streamlining Patch Management Processes and Incident Response Practices

Microsoft has made substantial progress in helping customers streamline their patch management processes and in enhancing our own practices with improved patch management tools, better patch delivery schedules and systems, and coordinated responses to vulnerability exploits. By working closely with our customers and partners, including federal government agencies and financial services firms, we have developed practices, processes and tools to help secure systems throughout the software lifecycle.

1. Enhancing Patch Management Tools

Microsoft actively participated in the National Cyber Security Partnership ("NCSP," www.cyberpartnership.org) task force on Security Across the Software Development Lifecycle; we helped to develop the NCSP's recommendations on patch management, which were released in April 2004. Our efforts to improve and streamline the patching process by enhancing the quality, accessibility, and ease of use of our patches and tools are consistent with those recommendations, and we are currently benchmarking our progress against them. Our efforts in this area have focused on:

- Improving the quality of our patches and our testing and release of patches.
  - Standardizing our testing processes with the goal of having a single company-wide testing process that delivers patches quickly and with consistently high quality.
  - Conducting a formal after-action review by the Microsoft Security Response Center ("MSRC") and the Secure Windows Initiative Team of any security patch so that we understand how the vulnerability occurred

and what changes are needed in the development process to reduce the likelihood of introducing such vulnerabilities in the future. We also identify any security response and patch-related problems so that they too can be rectified.

- Standardizing our patches' operation and standardizing the technologies they use, to provide users with a consistent, simpler patch experience.

- Working to make all patches reversible, in order to enable customers to "roll back" a patch if they encounter an unanticipated issue, such as a conflict between the patch and a legacy application.

- Ensuring that patches register their presence on the system in a consistent, standard way -- and producing improved scanning tools that make use of this registration information -- so users can quickly determine if their machines are patched appropriately.

- Providing a consistent patch release schedule, which currently is once a month. We will provide security bulletins and patches outside this schedule when necessary, such as when exploit code for a vulnerability becomes publicly available.

- Reducing the need to reboot systems after installing a patch, as our customers are more likely to apply a patch more quickly if server availability is not interrupted. In just the final six months of 2003, we reduced reboots by 10%.

- Reducing the size of the patches whenever possible to make it easier to distribute patches across low-bandwidth networks.

2. Patch Management Software

In addition to the enhancements above, Microsoft also offers patch management services and tools that can assist customers, regardless of their size, in conducting more effective patch management. Microsoft offers an online update service called Windows Update which can identify missing patches for the Windows operating system and install them automatically if the user elects to do so. Later this year, we plan to deploy Microsoft Update, which will perform the same functions as Windows Update for other major Microsoft software. Users may also obtain and install updates automatically through the Automatic Update feature included in recent Microsoft operating systems; in the future, automatic updating will be available for a wider scope of updates (including service packs, for example) and software (drivers and additional types of Microsoft software).

For businesses with straightforward patch management requirements, we also offer our free System Update Server ("SUS") patch distribution tool, which lets them, in essence, host their own Windows Update service for their companies. Windows Update Services ("WUS"), an enhanced version of SUS that will enable updating for additional Microsoft software lines as well as providing expanded automation and control capabilities, will be released soon. For customers who have more sophisticated needs such as the need to integrate patch management with application deployment and asset management, we offer System Management Server ("SMS"). Microsoft also offers a free

security scanning tool called Microsoft Baseline Security Analyzer which can scan for common system misconfigurations and missing security updates in Windows and other Microsoft applications.

Finally, we are developing advanced tools that will ease the management burden associated with managing updates. One example is called Strider, a tool that will help customers determine what level of interaction an update will have with their critical applications, thereby enabling them to tailor the amount of testing accordingly. By using Strider, customers will be able to identify the appropriate level of pre-deployment testing – a level that avoids unnecessarily lengthy and costly testing, while still giving them confidence that the update will work cooperatively with mission critical systems.

3. Microsoft Security Response Center and Emergency Assistance

Deploying state of the art patches and working with our customers to improve patch management processes are essential, but of equal importance is responding and communicating with our customers when vulnerabilities are discovered or there are issues that threaten our customers. MSRC is charged with providing this service by coordinating the investigation of reported vulnerabilities, the development of patches, and, together with our field teams, our customer outreach efforts. These outreach efforts include detailed security bulletins that provide information on the vulnerability, the risk it poses, and how to apply and manage the patch. In addition, Microsoft communicates with its customers through field bulletins, email outreach to more than one million subscribers, webcasts, outreach to the media and industry, and coordination with government agencies.

Should an attack or other extraordinary security incident occur, MSRC responds according to the protocols set forth in our Incident Response Process. Through this plan, we have honed our processes to rapidly mobilize Microsoft's worldwide resources when a worm like Blaster hits, to deliver information quickly to customers, and to help them protect their systems. The Incident Response Process also brings our engineering and communications departments together, enabling us to deliver the best information we can on defined timelines and to update that information at regular intervals.

The operation of the MSRC, our Incident Response Process, and our other efforts helped blunt the impact of the recent Sasser worm. Before the worm attacked, Microsoft had already significantly streamlined the patching process and launched the public awareness "Protect Your PC" campaign which led consumers to increasingly patch their systems. On April 13, 2004 Microsoft released a security bulletin and patch addressing a "critical" vulnerability. These and other efforts led to a 300% increase in the number of users who successfully patched their systems shortly after outbreak when compared with the Blaster experience.

Then, less than 24 hours after Sasser's discovery, we again contacted US-CERT with an alert and our perspective on the worm. Additionally, for those who could not patch in time, we provided, at no cost, a Sasser scanning and cleaning tool to identify the presence of the worm and remove it.

The existence of Microsoft's Anti-Virus Rewards Program encouraged individuals to provide information to law enforcement that contributed to the arrest of the Sasser author. Microsoft also worked with law enforcement, as we frequently do when

we or our customers are criminally attacked. We provide such assistance consistent with legal requirements and with respect for the privacy of our customers.

These actions, combined with the contributions of our partners in industry, the vigilance of our customers, our streamlined patching process, and the Engineering Excellence initiatives discussed below, helped the government and our customers worldwide to reduce the impact of Sasser on their systems and to limit or deter future attacks. Going forward, we are committed to continuing to meet the federal government's evolving security needs and to further improving our patch management processes.

B. Awareness and Planning

Microsoft's patches and tools rely in part on increasing awareness and education about good patch management practices and on individualized, appropriate patch management processes developed by our customers that take into account their specific mission, computing needs, system configurations, and user base. We continue to help our customers, including the federal government, to become more aware of vulnerabilities and defensive strategies and to develop effective patch management processes. Microsoft is working with key industry partners to help make federal agencies aware of security software and services that address the requirements of the Federal Information Security Management Act ("FISMA"). And through our Microsoft Services team, we mobilize security training in the field and help assess our customers' environments so that they may better prepare their systems and networks for inevitable criminal attacks.

II. Microsoft's Defense-In-Depth Strategy

While effective patch management and emergency response capabilities are vital to creating a more secure computing environment, Microsoft's defense-in-depth strategy goes well beyond these two aspects. The security pillar of our Trustworthy Computing initiative provides the overall framework and objectives for the defense-in-depth strategy:

- Secure by Design: Building security into the software from day one, by conducting threat modeling on software as part of the design stage, implementing that design faithfully and using solid coding techniques, and then confirming software security via architectural and code-level reviews;
- Secure by Default: Installing only minimal services by default, in order to reduce the attack surface area of our software;
- Secure in Deployment: Providing tools and guidance to help customers deploy systems more securely in production and to maintain that security through the system's lifetime; and
- Communications: Working with customers and partners to provide the fastest, most accurate updates on security issues.

Within this framework, we are pursuing a five-part strategy: Building technical innovations to provide greater Isolation and Resiliency on computers and networks, Authentication and Access Control improvements, Updating (discussed above),

Engineering Excellence, and, at the same time, providing security guidance to all of our customers, including federal agencies, and working with the government on public policy initiatives.

A. Engineering Excellence

As part of Trustworthy Computing, we are strongly committed to reducing vulnerabilities by using state of the art engineering practices, standards, and processes throughout the entire cycle of creating our software. We have undertaken a rigorous "engineering excellence" initiative designed to continue to advance the state of the art in software design, development, testing and release, and to keep our engineers trained in these techniques.

At Microsoft, we have formally integrated security into many of our software development processes through the Trustworthy Computing Initiative. We are designing and developing our software with security as one of our top priorities, and we have made security an integral part of the requirements that software must pass at various milestones in the development process. Essentially, security remains a constant focal point throughout software development.

Creating more secure software starts with a formal design process that verifies the security properties of the software at each well-defined stage of construction. The need to consider security "from the ground up" is a fundamental tenet of secure system development. Such a process is intended to minimize the number of security vulnerabilities injected into the design, code, and documentation in the first place and to detect and remove those vulnerabilities as early in the development lifecycle as possible.

From inception to release, a development team along with our central security team will evaluate the security of the software at each stage of development and testing.

Because new security threats constantly arise, we provide our software teams with updates on new threats and new defensive techniques. Training for our developers, testers, and Program Managers is a critical component of the Trustworthy Computing Initiative.

This improved development process has already resulted in a notable decline of vulnerabilities in some of our server software, and a corresponding reduction in the number of patches to be developed, tested, and made available to users. For example, the number of critical or important security bulletins issued for Windows Server 2003 during its first year in the market has been approximately one-third the number reported for Windows Server 2000 during its first year in the market.

B. Isolation and Resiliency

The traditional approach to security has been to design solid security into the platform and then reactively fix any bugs that are found. But we believe there is an additional step that could be taken – namely, improving protection against entire vectors of attack in an effort to protect the customer in the interim between discovery of the vulnerability and release of the patch. We are pursuing this level of protection by increasing system isolation and resiliency, with the goal of preventing malicious code from gaining a foothold on systems or limiting its effect.

Some of our major advances in increasing system isolation and resiliency are being included in our forthcoming Windows XP Service Pack 2. Those advances include:

- Increasing network protection by turning the Windows Firewall on by default, blocking all but desired networking traffic to a particular computer.
- Making use of a capability available in some chipsets to provide memory protection to help prevent exploitation of buffer overrun vulnerabilities.
- Providing better file attachment handling for email clients and instant messaging programs such as Windows Messenger. These email and instant messaging advances will significantly help reduce the risk of email viruses and worms.
- Reducing the threat posed by malicious code on web sites by preventing downloads from web sites except with explicit user approval.
- Altering how some network-aware services operate; for example, restricting by default a computer's response to remote procedure call requests unless the requester has been authenticated.
- Adding Windows Security Center, a feature that will provide centralized security management and monitoring functions and recommend guidance when action needs to be taken. This will improve security functionality by alerting users, via a pop up message, that their anti-virus software, for example, is off and providing them with an option for help.

Similar advances will be released for Windows Server 2003 in Service Pack 1. In addition, that service pack will include technologies that give IT administrators more control over how their servers are configured and stronger firewall protection for their networks.

A technology we have already delivered is client inspection, sometimes referred to as "quarantine," that can, for example, inspect PCs before they are given permission to connect to the network, to ensure they are patched and running an appropriately configured firewall. PCs that do not pass this inspection can be blocked and isolated from the network until they meet the corporate standards for safe access. The base capability of client inspection for VPN connections shipped in Windows Server 2003, and our research and development teams are looking at other protocols, beyond VPN, to determine how to advance this concept further and deliver it to customers.

Finally, we are developing what we call "Active Protection Technologies." Two of these technologies are Dynamic System Protection and Behavior Blocking. Dynamic System Protection refers to technologies that adjust the appropriate level of protection when an activity happens that affects a computer's susceptibility to attack. For instance, through Dynamic System Protection, a system might note that a particular update was not installed on the system, and automatically change some security settings to compensate. Once the patch is installed, the system will revert to its previous settings. In contrast, behavior blocking focuses on monitoring, identifying and intercepting code that acts suspiciously. User permission would then be requested before that code would be executed.

C. Authentication and Access Control

Another important focus for us is working with other industry leaders on next-generation technologies that control who gets access to networks and computers, and how they get that access. For example, working with industry partners, we have implemented authentication solutions, such as the 802.1x protocol, which significantly improves the security protections of a wireless network. This technology has now been included in Windows XP Service Pack 1 and Windows Server 2003. We have deployed this solution on our own network, a measure that has not only improved our own network security, but has also helped us develop deployment guides for customers.

Another such technology, built into Windows Server 2000 and 2003 and Windows XP, is IPSec. IPSec protects private data in a public environment by encrypting all network traffic and requiring authentication at the individual computer level. As a result, it sets a much higher bar for network access, making it harder for outsiders to eavesdrop and representing a dramatic improvement in network security. Again, deploying this technology on our network has helped us to understand the technology better, to help customers deploy it widely within their networks, and to develop prescriptive guidance for customers such as the US Air Force, which has successfully deployed IPSec on its own networks.

Finally, Microsoft continues to work with industry partners to increase use of smart cards and other emerging, highly secure two-factor authentication techniques, and to develop future technologies that allow a computer to recognize and identify an individual with greater confidence.

D. Security Guidance

All the foregoing technologies, however, will not realize their full potential unless our customers, including federal agencies and their employees, have the information and training necessary to exercise appropriate security choices. That is why Microsoft has partnered with the federal government on cyber-security issues, invested in education initiatives, and provided security tools and resources on the Microsoft web site.

1. Partnering With Government

Part of Microsoft's efforts at providing security guidance is directed at working with the federal government to protect its own computing environment and the country's critical infrastructure. For example, Microsoft has partnered with the Department of Homeland Security ("DHS") on two fronts. First, Microsoft has been working with DHS' National Cyber-Security Division to raise awareness of cyber-threats through the release of prompt security bulletins. And second, Microsoft has been working with DHS and other industry leaders in efforts to help foster sharing of security information within the homeland security community.

Microsoft has also been assisting the National Institute of Standards and Technology ("NIST") and the National Security Agency to develop IT security guidelines in areas such as minimum security standards and Windows operating system deployment guides for government agency systems. Those guidelines are expected to assist federal agencies in complying with NIST-developed standards which are to become mandatory in 2005. Further, Microsoft remains committed to meeting the standards set forth in the Common Criteria. Currently Windows 2000 has achieved the highest

Common Criteria certification achieved by commercial software (EAL 4), and we are now seeking certification for Windows XP, Windows Server 2003, Exchange Server, and SQL Server.

Finally, Microsoft officials have served as advisors to the President on policy and technical issues associated with information technology, cyber-security, and technology through participation in such organizations as the National Security Telecommunications Advisory Committee and the President's Information Technology Advisory Committee.

2. Education Initiatives

In addition to partnering with government, Microsoft has also worked with other industry members and acted on its own to improve cyber-security awareness. For example, Microsoft has joined forces with industry members and groups such as the Consumer Federation of America, the National Consumers League, Consumer Action, and the National Cybersecurity Alliance, which is supported by both DHS and the Federal Trade Commission, to promote security education.

Microsoft also is undertaking a Security Mobilization Initiative that includes in-person labs hosted by Microsoft-certified trainers to develop real-world security skills, one-day security summits and forums, and narrated security slides and demonstrations on our web site. The goal of the Initiative is to reach 500,000 business customers by the end of this year with information on how to configure and protect systems and networks to increase security. We are in the process of hosting 20 security summits around the country, including one that recently took place here in Washington D.C. on April 8, 2004. This builds on the long history of similar events Microsoft has sponsored with the federal

government, such as the biannual Government Security Summits we have hosted for the last seven years in both Washington D.C. and Redmond.

3. Microsoft.com Security Guidance

Finally, Microsoft.com offers an array of guidance forums to educate users on cyber-security. For example, we host monthly web chats where customers can ask questions relating to security in Microsoft software. Microsoft.com also hosts the Microsoft Security Developer Center where IT professionals can obtain a variety of educational materials and best practices for securing their systems. From there one can quickly reach the Security Guidance Center, which offers professionals the technical guidance, tools, training, and updates needed to assist in planning and managing a security strategy that is well-suited for their organization. Finally, Microsoft offers additional assistance in a variety of formats, including technical chats between Microsoft customers and Microsoft technology experts, Security E-Learning Clinics, and security newsletters.

E. Public Policy

Security is one of our top priorities; we have a tremendous amount of activity underway and are experiencing measurable success. Yet this is an area where we all have roles to play, including the government. As the Congress and the Administration address cybersecurity, we suggest the following actions:

First, we hope the Senate will ratify the Council of Europe Cyber Crime Treaty to help streamline international criminal investigations.

Second, our law enforcers are doing great work, and need more training and better equipment at all levels to help them investigate and prosecute cyber crimes effectively and thoroughly.

Third, government systems administrators would benefit from more intensive training in security.

Fourth, government participation in consumer education campaigns will help raise awareness about the criminal threats and the necessity of ongoing system protection.

Fifth, the NIAP/Common Criteria process is working and should be the primary information assurance certification process for government systems. We support reforms to make NIAP more efficient and cost-effective.

Finally, we support strongly increased basic research in cybersecurity and computer forensics.

We are eager to work with the government in each of these areas.

Conclusion

We continue to pursue our Trustworthy Computing initiative, to improve our patch management processes and tools, and to assist our customers in developing and maintaining a multilayered approach to securing their systems. In the final analysis, a more secure computing environment is best achieved when industry leaders continue to innovate around security and work closely with their customers to help them keep their software up to date, configure their networks properly, train their IT staff to manage the

network appropriately and perform necessary maintenance activities, and benchmark their activities against security and patch management policies.

Mr. PUTNAM. Thank you.

Our next witness is Louis Rosenthal, executive vice president, ABN AMRO Services Co. He is responsible for information technology infrastructure and operations, supporting the consumer, commercial mortgage and e-commerce business units of ABN AMRO in North America, as well as some global business units.

Prior to his current position, Mr. Rosenthal held the position of executive vice president of service delivery at European American Bank in New York, formerly owned by ABN AMRO. Prior to that, he spent 7 years at the Bank of New York. He serves on the executive committee and advisory group for BITS, the technology arm of the Financial Services Roundtable.

Welcome to the subcommittee. You are recognized for 5 minutes.

Mr. ROSENTHAL. Thank you, Mr. Chairman, for the opportunity to testify today about the ways the financial services sector is addressing information security challenges.

I am Louis Rosenthal, executive vice president with LaSalle Bank Corp., a subsidiary of ABN AMRO Services Co. I am pleased to appear before you today on behalf of BITS and the Financial Services Roundtable. I am a member of the BITS Executive Committee, a non-profit industry consortium of 100 of the largest financial institutions in the United States. BITS is the sister organization to the roundtable. LaSalle, one of the largest banks in the midwest, is a subsidiary of Netherlands-based ABN AMRO Bank operating in about 60 countries around the world with about $780 billion in assets.

Through BITS, the financial services industry has been at the forefront of advancing security. No industry takes cyber security more seriously than the financial sector. The financial services industry is firmly committed to safeguarding our customers' information, maintaining our trusted relationship with our customers and complying with the numerous laws and regulations promulgated by the financial regulators.

The challenges are plentiful. As I speak, hackers are writing code to compromise systems. Viruses are at epidemic levels. We are increasingly concerned that a coordinated cyber attack of some kind could impact communications, SCADA systems or first responder systems and put all of us at terrible risk. The prospect of zero day exploits with malicious payloads are a reality. Cyber security, like physical security, is critical to the well being of the Nation and its infrastructure.

Financial institutions are heavily regulated and constantly supervised by our Federal and State regulators. The industry has worked consistently and diligently to comply with these requirements. We do not believe more regulation of the financial services industry will help us address the cyber security challenges. Rather, we believe the private and public sectors must work together to address cyber security issues. That is why we are urging our partners in the technology industry to do their fair share to ensure the soundness of our Nation's critical infrastructure. It is also why BITS enthusiastically participated in the chairman's Corporate Information Security Working Group.

Ensuring software security is enormously costly. In December 2003, BITS surveyed its member institutions on the cost of ad-

dressing software vulnerabilities, including managing software patches. We found that software vulnerabilities are approaching the cost of $1 billion annually to the financial services industry alone.

In October 2003, BITS launched its software security and patch management initiative. BITS' goal is to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management and help member companies comply with regulatory requirements.

A key part of this work is our collaboration with software companies to create solutions acceptable to all parties. We have shared with these companies a series of business requirements that BITS members agree are critical to the soundness of systems used in the financial services industry. In February of this year, BITS and the Financial Services Roundtable held a cyber security CEO summit here in Washington. The event promoted CEO to CEO dialog on software security issues.

This past April, BITS and the Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. BITS is working with other critical infrastructure industries and industry associations to help motivate a larger user movement. For example, BITS worked closely with the Business Roundtable in developing that organization's widely publicized cyber security principles. The BITS Product Certification Program is another important part of our work to address software security. The BITS Certification Program is a testing capability that provides security criteria against which software can be tested.

It is important for the committee to recognize the dependence of all critical infrastructures on software and the Internet. In so doing, we have developed six key recommendations for the committee to consider. One, encourage providers of software to accept responsibility for their role their products and services play in supporting the Nation's critical infrastructure. Two, support measures that make producers of software more accountable for the quality of their products including ensuring their products are designed to include security as part of the development process, testing that their products meet quality standards and that financial services security requirements are met before the products are sold, developing patch management processes that minimize cost, complexity, downtime and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested and continuing patch support for older but still viable versions of software currently in use in the critical infrastructures.

Three, provide incentives and other measures that encourage implementation of more secure software development processes. Four, provide exemption from antitrust laws for critical infrastructure industry groups so they can better discuss and develop baseline security requirements for the software and hardware they purchase. Fifth, encourage collaboration and coordination among other critical infrastructure sectors and Government agencies to mitigate software security risks. Sixth, encourage regulatory agencies to re-

view software vendors similar to how the regulators currently review third party service providers so that software vendors deliver safe and sound products to the financial services industry. Through collaboration and a partnership, we can address the cyber security challenges.

Thank you for the opportunity to testify today and I will take questions later.

[The prepared statement of Mr. Rosenthal follows:]

STATEMENT

OF

LOUIS F. ROSENTHAL
EXECUTIVE VICE PRESIDENT
LASALLE BANK CORPORATION

ON BEHALF OF
BITS AND THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

UNITED STATES CONGRESS

HEARING ON
INFORMATION SECURITY—
VULNERABILITY MANAGEMENT STRATEGIES AND TECHNOLOGY

JUNE 2, 2004

TESTIMONY OF LOUIS F. ROSENTHAL
EXECUTIVE VICE PRESIDENT, LASALLE BANK CORPORATION

Introduction

Thank you, Chairman Putnam and Ranking Member Wm. Lacy Clay, for the opportunity to testify before the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census about the ways the financial services sector is addressing information security and our strategies and technologies for managing vulnerabilities.

I am Louis F. Rosenthal, executive vice president, LaSalle Bank Corporation. I am pleased to appear before you today on behalf of The Financial Services Roundtable (The Roundtable) and BITS. LaSalle is one of the largest banks in the Midwest and second largest in Chicago, serving individuals, small businesses, middle market companies and institutions. LaSalle Bank Corporation is a subsidiary of Netherlands-based ABN AMRO Bank N.V., one of the world's largest banks with total assets of EUR 639.9 billion (781.7 billion USD) and a presence in more than 3,000 locations in over 60 countries.

I am also a member of the Executive Committee of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the US. BITS is the sister organization to The Financial Services Roundtable. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. BITS is not a lobbying organization. Our work in crisis management coordination, cyber security, critical infrastructure protection and fraud is shared not only among our member companies but throughout the financial services sector. BITS works with other critical infrastructure sectors, government organizations, technology providers and third-party service providers to accomplish its goals.

Information security is a complex challenge. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so vital to the stability of

financial services and the strength of the nation's economy. At the same time, we are a favorite target of criminals operating in cyberspace and of terrorists, as was made clear on 9/11.

Through BITS, our industry has been at the forefront of advancing security in financial services. However, all interested parties in the private and public sectors must work together if we are to address these issues sufficiently. I would like to recognize and thank Chairman Putnam and subcommittee staff for their outstanding work on public-private information security partnerships, particularly for leading the Corporate Information Security Working Group. You understand, as we do, that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

Financial Industry Perspective

Ensuring software security is enormously costly for the financial services industry. In December of 2003, BITS surveyed its members on the cost of addressing software vulnerabilities, including managing software patches. We found that:

- Software vulnerabilities are approaching a cost of $1 billion annually to the financial services industry.
- BITS and Roundtable member companies pay an estimated $400 million annually to deal with software security and patch management issues.
- Just managing patches—which is only a fraction of what we do to deal with vulnerabilities—costs BITS and Roundtable members an estimated $55 million annually and costs the industry an estimated $110 million annually.

The inadequate levels of security within the software our industry purchases, coupled with current inefficient software-patching processes, cause our industry to spend millions of dollars that could be better used for other purposes such as enhancing security and business-continuity practices and offering products and services at lower cost to our customers.

This is an alarming issue and critical to protecting the nation's infrastructure. As I speak, hackers are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus. They are employing the tactics of spammers to rapidly spread their destructive code globally. We are increasingly concerned that a coordinated cyber attack of some kind could impact communications, Supervisory Control and Data Acquisition (SCADA) systems, or first responder systems and put all of us at terrible risk.

The problems are worsening. Attacks on all types of businesses are escalating. Financial services companies are a particularly attractive target. The Deloitte Global Security Survey 2004 finds that the majority of global financial institutions have seen an attack on their IT systems within the last year, and that many of those breaches resulted in financial loss. Eighty-three percent of respondents reported their systems had been compromised in 2003, versus 39 percent in 2002.

As you know, financial institutions are heavily regulated and actively supervised by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. With the substantial risks of software security, regulators are stepping up their oversight even further. Our industry is working consistently and diligently to comply with new regulations. However, regardless of how well institutions respond to regulations, we simply cannot address these problems alone. Our partners in the software industry must also do their fair share to ensure the soundness of our nation's critical infrastructure.

Financial Industry Efforts

Consumer trust is essential to the success of all US financial institutions. Central to BITS' mission is sustaining that trust. BITS has been advancing security in the financial services industry since its inception in 1996. The BITS Security and Risk Assessment (SRA) Working Group, for example, represents more than 70 of the nation's largest banking, securities and insurance organizations.

The SRA has evolved to meet the increasingly important information security issues of our members and the industry. In October of last year, BITS increased its focus on flawed software with a Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. BITS' goal with this work is to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management caused by vendor practices, and help member companies comply with regulatory requirements.

BITS is working to encourage a higher "duty of care" by software vendors that sell to critical infrastructure industry companies, to promote compliance with security requirements before software products are released, and to make the patch-management process more secure and efficient and less costly to organizations.

Also in October of 2003, BITS began forging partnerships with the vendors of software most commonly used in our industry. In February of 2004, BITS and The Financial Services Roundtable held a Cybersecurity CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. More than 80 executives from financial services, other critical infrastructure industries, software companies, and government discussed software vulnerabilities and identified solutions. A "toolkit" with software security business requirements, sample procurement language, and talking points for discussing security issues with IT vendors was distributed to 400 BITS and Roundtable member company executives. A theme of the event was the importance of collaborating with other critical infrastructure industries and government. Since the Summit we have worked with all the associations representing the financial services industry, The Business Roundtable and some sector-specific associations.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. We are also seeking protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase. Additionally, as part of the policy, BITS and the Roundtable are encouraging regulatory agencies to explore supervisory tools to ensure critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry.

Today, we are working with software companies to create solutions acceptable to all parties. We have provided these companies with a series of business requirements that BITS members agree are critical to the soundness of systems used in the financial services industry.

BITS is also working with other critical infrastructure industries and industry associations to help motivate a larger user movement. Most recently, BITS' consultation and collaboration with The Business Roundtable resulted in that organization's widely publicized response to the state of software security. The Business Roundtable called on software producers and end users to work together to build a more unified defense against the increasing number and growing cost of cyber attacks.

The BITS Product Certification Program is another important part of our work to address software security. The BITS Product Certification Program is a testing capability that provides security criteria against which software can be tested. A number of software companies are considering testing. The criteria are also used by financial institutions in their procurement processes.

This summer, BITS will publish best practices for patch management from the user's perspective. As I mentioned earlier, patch management and implementation alone can cost one financial institution millions of dollars annually. Cost aside, it is critical for patches to be prioritized, and implemented as quickly as possible, given the speed with which viruses are targeting new vulnerabilities.

We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing software security and vulnerability management.

Recommendations

We have developed six key recommendations for the Committee to consider:

1. **Encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure.** Software providers need to exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.
2. **Support measures that make producers of software more accountable for the quality of their products.**
    a. Ensure their products are designed to include security as part of the development process.
    b. Test that their products meet quality standards and that financial services security requirements are met <u>before</u> products are sold.
    c. Develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
    d. Continue patch support for older, but still viable, versions of software.
3. **Provide incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation**

of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.

4. **Provide protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.**
5. **Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to mitigate software security risks.**
6. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers—so that software vendors deliver safe and sound products to the financial services industry.**

It is important for the Subcommittee to recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the nation's critical infrastructures, needs to be explored. Further, the Subcommittee should recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

On behalf of LaSalle Bank Corporation, BITS, and The Financial Services Roundtable, thank you for the opportunity to testify before you today. I will now answer any questions.

Mr. PUTNAM. Thank you, Mr. Rosenthal.

Our next witness is Marc Maiffret, chief hacking officer for eEye Digital Security, a leading security software provider. In 2001, eEye engineers discovered and named the Code Red virus and helped the White House avert a potential disaster. In addition, eEye's research team discovered the latest Microsoft ASN vulnerability.

Mr. Maiffret has been featured in several publications and has testified previously before Congress providing his expert opinion on the Nation's infrastructure.

Mr. Maiffret, welcome to the subcommittee. You are recognized for 5 minutes.

Mr. MAIFFRET. Thank you very much.

For some time, security has been a race to create new protection mechanisms for never ending onslaught of vulnerabilities, the vulnerabilities that organizations face are not simply system and software vulnerabilities but also social vulnerabilities and how people interact with technology.

On the surface, it would seem the simple solution to the vulnerability problem would be as easy as organizations patching their systems. This however is not the case. Times are changing and now more than ever new threats arise quicker than ever before. The window of vulnerability which is the time organizations have to patch the systems is shrinking.

On average, new threats emerge between 1 and 2 weeks after a vulnerability is discovered, therefore not allowing companies to react fast enough. Patching is not enough. We need new security solutions that can mitigate the risk of vulnerabilities before new threats emerge regardless if systems are patched or not.

One of the reasons that organizations are failing is not from a lack of security tools but from the lack of creating a process and policy around those security tools. Simply having the tools to know that you are vulnerable or that you are under attack is not enough if the information is not audited and tracked to some sort of completion.

I thought it would be helpful to illustrate in kind of real world terms some of the problems that a large organization actually faces in terms of computer security. I actually met with the head of security for the largest financial organization in the United States and have some interesting statistics. This organization is actually in charge of auditing 2.5 million IP addresses or computer addresses. Out of those 2.5 million IP addresses, there is roughly over half a million active systems or computer or devices they need to protect. On a system of this scale, there is really no room for failure, even if you think of a 1 percent failure of security or a 1 percent failure of patches being deployed and whatnot, that is still many thousands of systems potentially going to be at risk or no longer functioning. Those are systems that are dependent for business processes and other types of activities.

The interesting thing is that while some of these numbers are staggering for this organization, they are able to maintain their security in a way that allows them to not only roll out patches within 48 hours of vulnerabilities being released, but at the same time

have all the right protection mechanisms in place on the perimeter of their network.

Even with all this, being a large network and having a good response to security, doing everything right is costing them roughly $15 million per security incident. That would be a critical security vulnerability which requires them to go out of the normal operation activities to deploy a patch or to secure their systems.

That is all I have for now.

[The prepared statement of Mr. Maiffret follows:]

June 2, 2004

Marc Maiffret
Chief Hacking Officer
eEye Digital Security

Congressional Subcommittee Testimony on Security Threats to Public and Private U.S. Infrastructure

Vulnerability Management Strategies and Technology

For some time, security has been a race to create new protection mechanisms for a never-ending onslaught of vulnerabilities. Vulnerabilities are at the core of what makes systems insecure. However, the vulnerabilities that organizations face are not simply system/software vulnerabilities, but also social vulnerabilities in how people interact with technology. Until not long ago most organizations were winning the security race, because the "bad guys" were letting them. Things have changed though, attackers have become smarter, and the race is over. The "good guys" have lost, for now, and there has never been a better time to be a criminal.

One of the main reasons for the "good guys" losing this battle is due to the fact that security has always been reactionary. With the current trends in vulnerabilities, there is no time to react. It is important to emphasize the reactionary state of security to help better understand the dynamics of why we are failing.

Patches Aren't Always The Answer

If you casually look at the available studies and statistics you can easily point the blame at organizations for not patching their systems. Then again, you can also read newer studies which say patching is not enough - you cannot patch in a reasonable amount of time before new threats emerge (worms, viruses, exploits, etc.). Others say that it is not a problem of not patching or not patching fast enough, but there is an increase in "zero-day" vulnerabilities or threats that take advantage of non-public vulnerabilities which do not yet have patches. Keeping all of these dynamics in mind, you have to realize that the threat of vulnerabilities, which can be fixed through patches, is only one of a few different types of vulnerabilities that organizations face. Organizations are also vulnerable to various software/system configuration vulnerabilities, as well as social vulnerabilities.

Misconfigurations and social vulnerabilities are the most publicized types of attacks, and also the least. Virus attacks are one form of social vulnerability that is typically made very public. Viruses are able to propagate from system to system based on human interaction with software in a way that is harmful to the system the software is running on. The problem then escalates from one infected system to entire companies and groups of computer users. There are other types of vulnerabilities in software and systems that can be leveraged by attackers who take advantage of misconfiguration weaknesses in order to gain access to resources that attackers shouldn't otherwise have

access to. One recent example of this is when internal memos from the Senate Judiciary Committee were compromised. I'm sure you're all familiar with that particular instance. A solid Vulnerability Management plan will also cover the aspects of policy and compliance, user education and various other security facets beyond simple patch remediation.

Security According to Specific Needs

Vulnerability management should be at the heart of every organization's security strategy. Most organizations would love to have the single silver bullet for vulnerability management. While security companies will all claim that they offer it, there is no one solution. Instead, one of the most important aspects of creating a good vulnerability management plan is to first understand what is critical within your organization. From the private sector to the public, from financial services to health care, there are many differences in what is critical within an organization, and therefore different security requirements.

One of the first things to accept in securing a large enterprise is that the odds of being impervious to attack are against you. This is as good as a drunken road-trip to Vegas and betting your next house payment on black. There are no two ways around it; the odds that there will always be a way for a hacker to penetrate your network are against you. That is why it is important to understand what is critical within your organization and focus on those critical points first, before trying to tackle the security of your organization in its entirety. Obviously there are various levels of security a company can obtain, and with that, there are various layers of security that are required to advance to the next level. To understand what layers of security are required for your organization to reach various levels of security, you must first understand the types of threats your organization could possibly face.

Imagine for a moment that there are potentially thousands and thousands of people who live for "the thrill of the hack." From the young boy working all hours of the night to find that next vulnerable system to the next virus writer hoping to see their work made public around the world, there are many different types of computer criminals, and for the most part none of them seem to care which computers they target. Now take that image of computer "criminals" and never think of it again. Times have changed. Though some things have remained the same, the motivation and people behind computer intrusions has drastically changed.

As with any "free" and open system (computers, networks, Internet, etc.), that relies heavily on trust, the fun has to eventually come to an end. The "bad guys" have grown all too knowledgeable about the fact that technology is creating new opportunities to profit and proliferate from the same common criminal ideas that have existed for many years. This is all very evident by the investigations into various online fraud activities performed by the Federal Bureau of Investigation, many of which lead back to various countries where organized crime is able to operate more freely because of lax computer security laws and poor relations with the United States. There are other attacks, beyond simple online fraud, that are more sophisticated. Attacks that target specific companies and leverage things unique about an organization in order for an attacker to acquire whatever it is they are after. Regardless, if you want to believe the "boogeyman" stories

of organized crime or foreign nations breaking into your computer networks, the one attacker that almost all organizations have met with face-to-face is the computer worm.

A computer worm is a program that leverages a "vulnerability" (typically found in software) to replicate itself from one computer to another without requiring any human interaction. Depending on the computer worm, there is sometimes a "payload" that is included with it. Payloads can be anything from malicious code that uses thousands of worms to create a coordinated attack against a target system, or a payload could simply attempt to disrupt or destroy data on infected systems. While the idea of computer worms sounds scary, the idea is nothing new.

Computer worms have been around for some time now. However, they are becoming more and more popular and seemingly easier to produce than ever before. One of the first known records of a computer worm stems all the way back to 1988 when Robert T. Morris Jr. released the first computer worm, seemingly by accident. One interesting aspect of the first computer worm was not specifically about the worm itself but more so about the author. The father of Robert T. Morris Jr., at the time the worm was released, was none other than Robert Morris who was then the Chief Scientist of the National Security Agency (NSA). Some would later speculate whether or not Robert T. Morris Jr. came up with the concept of the computer worm on his own. While there is interesting mystique surrounding the first computer worm, we must remember one thing. The first computer worm was written over 16 years ago. We have had 16 years to think about, analyze and create solutions to guard against computer worms. So why after all of this time, are businesses constantly impacted by computer worms? More so, why are businesses still impacted by vulnerabilities?

Vulnerabilities Are Typically A Known Quantity

Vulnerabilities in software and systems are what allow computer worms to propagate in the first place. When a vulnerability is discovered, typically that vulnerability is reported to the manufacturer of the software in which the vulnerability is found. At that point, the software vendor begins to assess the risk that the vulnerability poses to its customers. In some cases, the vendor also assesses the risk of embarrassment they will endure in the media. After some time, the vendor will eventually release a security patch and security bulletin to notify its customers of the new risk and that they need to apply the relevant patch. Parallel to that, the security researchers who discovered the vulnerability will also release a security bulletin that describes the vulnerability and gives possible mitigation information that can be put in place until a patch is deployed. At this point, a vulnerability has been made public. From the patch itself, enough knowledge has been disseminated that allows attackers to create worms and exploits, or programs that can take advantage of a vulnerability to compromise computer systems running the vulnerable software. This is when security starts to fall apart in the vulnerability life cycle. The reason being, vulnerabilities are being exploited faster than organizations are able to react to them and patch their systems. Therefore, even the most security-astute organizations are still going to be impacted by worms and computer attackers.

Some people have equated the current "vulnerability lifecycle" in relation to the term OODA Loop, or Observation Orientation Decision Action Loop, which was first

coined by Col John Boyd, USAF (Ret). In relation to vulnerabilities, the idea of the OODA Loop is that if an attacker can get "inside" your OODA Loop they will have the upper hand, as organizations will not be able to properly respond to attacks and instead be left in a helpless and disoriented state. All analogous jargon aside, if exploits and worms are being released before organizations can react, organizations will continue to be impacted by the ever-growing number of threats.

Coming around full circle we know that having good vulnerability management means good security policy and compliance, user education and technologies that will allow your organization to regain control of the vulnerability lifecycle. There are many technology solutions and service providers that cover the various areas of vulnerability management. One of the first steps an organization must take is determining a trusted source to help them along their path of creating a good vulnerability management plan. Many organizations actually do have a wealth of security knowledge within them just waiting to be tapped into. An outsider's perspective can also be helpful for organizations in determining their current security stance and critical business processes.

Angles Of Vulnerability Management

When it comes to vulnerability management, there are a few basic technologies with varying levels of sophistication. Most of the technology related to vulnerability management can be separated into two functional groups: perimeter and endpoint, or host-based, security. There is, however, one technology that plays an important part in both perimeter and endpoint security - vulnerability assessment. The first place that companies typically make an investment in security is around the perimeter of their network.

Perimeter security is one of the older forms of security which for many years has been made up of two main types of security solutions: firewalls and Intrusion Detection Systems. Firewalls were created to provide access controls on how systems are allowed to communicate with one another. While firewalls worked very well for their intended purpose, they eventually were not enough to handle all the new emerging threats. Based on that line of thinking, the idea of the Intrusion Detection System (IDS) was born.

IDS created a way to monitor all network communications for various attack patterns and then create notifications based around those attack patterns. Those notifications were then interpreted by an organization's IT staff to determine whether or not a system really had been compromised. This technology is no longer a viable option as most organizations have realized that IDS requires too many personnel resources without much return on investment. From this failure and various market analysts proclaiming, "IDS is dead," there was the birth of Intrusion Prevention Systems (IPS).

IPS is the next wave of perimeter security that aims to protect organizations from both known and unknown attacks. Unlike IDS, IPS is supposed to actually stop attacks, and not just notify organizations about them. Therefore, giving an increased level of security by blocking attacks around the perimeter of your network. The problem though is that many IPS solutions are nothing more than repackaged IDS solutions that have been repurposed to "block attacks" instead of just notifying organizations about attacks.

One of the fundamental flaws of IDS/IPS systems, regardless of whether or not they are able to block attacks, is that they protect against exploits and worms which are not necessarily the core of the security problem organizations face. Again, the core of the security problem is the vulnerabilities. Since IDS/IPS systems are protecting from exploits and worms, the threats, and not vulnerabilities specifically, they fall into the same vulnerability lifecycle trap that was described earlier. Again, your security is only as good as how quickly your IDS/IPS system can be updated. You might have gained a little bit of time in the race against attackers; however. in most cases you still have not gained enough time to win the race. In general, firewalls, IDS and IPS, do have their applicable uses and every company should, at the very least, be investing in perimeter security. It should, however, be understood very clearly that perimeter security is not enough. One of the reasons why perimeter security, no matter what kind (firewall, IDS, IPS, etc.), is not enough is because the dynamic nature of threats and business processes has created a plethora of ways that attackers, worms, etc. are able to find their way inside an organization's network.

Companies who have invested heavily in perimeter security are still being affected by various security threats for a few reasons. One of the reasons is that of remote and rogue computer users. Whether it's a user traveling with a laptop on the road or logging in from home, all too often, remote users' machines are being infected with worms, or "back-doored" by attackers. Eventually those remote users bring their systems back inside the organization, at that point, bypassing any perimeter security that is in place. Remote and rogue users are not the only ways perimeter security is being unknowingly bypassed these days. Other breaches in perimeter security are commonplace in relation to business processes that require two organizations to communicate between one another, often times from within each organization's perimeter. From these various deficiencies in perimeter security came the idea of endpoint security solutions.

Endpoint Security

Endpoint security will receive a great deal of attention over the next few years. This is because endpoint security solutions are providing security at the closest point to the digital assets that organizations are trying to protect. There are many types of endpoint security solutions and many of them are similar, if not identical, to some perimeter security solutions. Patch management solutions are also a part of endpoint security and are growing in popularity.

No one can deny that one of the most crucial things an organization needs to be doing for security is installing the latest security patches. There are many adequate solutions on the market today that allow for organizations to deploy patches across their environment with relative ease. When looking at patch management solutions, organizations need to be careful about the scalability of certain patch management solutions. While a patch management solution might seem like a great idea in concept or in a lab, many patch management systems start to break down and have problems when they are used on a network of any sort of large scale. Another deficiency in most patch management solutions is that their management capabilities, beyond even scalability,

have not been built with large organizations in mind. Patch management and remediation is not as simple as clicking a button and blasting a patch out to all the systems that need it, although that's how most patch management solutions work. Patch management is very much process-related, and the process of deploying patches changes depending on each organization. Even a scalable and process-oriented patch management solution is not going to be enough to protect your organization. Again, the current vulnerability lifecycle does not allow organizations enough time to patch before a new threat emerges. That does not mean you should not be looking into patch management or patching your systems...just don't bet the farm on it.

One security technology that has been pioneered recently has been that of Endpoint Vulnerability Protection. Endpoint Vulnerability Protection works by being able to understand the vulnerabilities that are used by exploits, worms and attackers. By truly protecting systems from vulnerabilities and not threats, EVP systems are able to protect systems automatically from new threats, before they arise. That is to say that when a vulnerability is released, an EVP system is then able to specifically protect a system from that vulnerability. So no matter what new threats, worms or otherwise, are released, your systems will already be protected ahead of time; therefore, giving you the advantage in the vulnerability lifecycle. This then allows you to deploy patches throughout your organization when it makes sense for your business. Your systems remain protected even without patches installed.

While endpoint security in some ways sounds like the silver bullet to security you must keep a few things in mind. First, there are many different types of endpoint systems that organizations need to protect: Windows, Linux, Apple, Unix, routers, and various other devices. Most endpoint security solutions do not offer support for all of these different platforms, and some platforms are simply impossible to create endpoint security solutions for, as they are proprietary. Also, endpoint security solutions are only going to protect systems that organizations know about and systems on which they can install endpoint agents. There is still the threat of rogue machines, machines that cant run the endpoint agent software, and various other instances where endpoint security is not applicable. These are just a few of the reasons that some of the largest organizations in the world rely on one of the oldest type of vulnerability management tools ever created: vulnerability assessment.

Vulnerability assessment is a solution that can provide organizations with a clear view of their current security stance, whether it is perimeter security, endpoint security, rogue devices, or security policy compliance. Vulnerability assessment allows you to view the security of your network from all angles and create a real-world view of how your organization is doing in terms of its risk to malicious attackers. Years ago, Vulnerability Assessment (VA) was mostly thought of as a quick-use security-consulting tool, and for the most part it was. Over time, VA solutions have evolved into enterprise-class security solutions that provide companies the real-time information they need to properly assess their security posture when new threats are discovered. Beyond that, VA solutions have evolved into more process-centric solutions that allow organizations to track vulnerabilities from their initial discovery all the way through their remediation. This allows organizations to have a better understanding of the types of vulnerabilities

they are facing, as well as management of the personnel and resources that are required to ascertain various levels of security.

One of the last technological building blocks of vulnerability management is a solution to manage the many processes that make up vulnerability management. Whether it's your perimeter security, endpoint intrusion prevention, or patch remediation, the various solutions for vulnerability management alone are not enough. Having the various tools to perform vulnerability management does not necessarily mean you have created the business processes to verify that everything is in compliance to your set standard. The end-to-end vulnerability management plan should include a solution to manage the process as a whole. Simply having vulnerability assessment, firewall, patch remediation tools, etc. is not enough. You need to have a process to track your organization's progress and verify that you are at some level of compliance relative to your business goals. Organizations must also remember that one of the most important natural resources and backbones of security and vulnerability management is the security researcher.

Security researchers come in many forms from the hobbyists staying up all hours of the night finding security bugs for fun to the paid employee working for a security companying researching new vulnerabilities. No matter what type of security researcher, security researchers are critical assets in helping organizations gain a level of security. That is not to say every organization must have their own security researchers on staff, but organizations must remember that by wanting their systems to be secure, they are in part joining a security community made up of all types of people. Organizations must be wise in knowing what people and movements/ideas they should support. There are many battles that are waged between big business and the security researcher. The majority of time "big business" is the very companies who are writing insecure software and putting organizations/customers at risk, who would rather security researchers went silent. If no one talked about the problem, then there wouldn't be a problem.

Thinking Like A Criminal, For Greater Security

Looking to the past we can find instances where battles were staged. Organizations, researchers, companies, and even government, all took sides on debates about security. Had some of these debates gone truly sour, we would have seen a rippled effect that would have caused a giant set back to the security of organizations today. So what was one of these historical turning points where community decisions on security could have caused things to go horribly wrong? The birth of vulnerability assessment. One of the very first vulnerability assessment tools ever created was SATAN. When SATAN (System Administrators Tool for Analyzing Networks) was first created many organizations and institutions went into a bit of a panic. Some people got the idea in their head that the creation and public release of vulnerability assessment tools would allow for the "bad guys" to use the tools against organizations and therefore help the "bad guys" in their efforts to break into systems. The creators of the tool argued that the tool was needed by the "good guys" in order to be able to identify all the ways that the "bad guys" could break into systems and have information on how to fix those insecurities. The creators believed so strongly that they were doing what was right for security that at least one of the creators put their professional career at risk. A long time

before SATAN was created, "bad guys" had been using these types of tools to break into computer networks, but the "good guys" were never clued in to have the same tools as the "bad guys." The idea of thinking like a criminal, to stop a criminal seemed a hard pill to swallow at the time. If you look at present day security you will see that vulnerability assessment tools are very common-place within organizations and are widely accepted as being one of the greatest network security tools. This is just one example that hopefully illustrates the need for organizations to stay in touch with security researchers, their ideas and their motivations. Where would organizations be now if vulnerability assessment tools had been outlawed? Where will organizations be tomorrow if free thinking and publication of vulnerability research and exploits were outlawed? Shouldn't we be more concerned, first and foremost, with the accountability of companies creating the insecure software? When the battle is waged between researchers and software vendors for accountability on both parties' parts (researches for their information and software vendors for their insecure software) where will your organization stand? Or will you not be informed enough to lend a hand in making sure computer security keeps progressing ahead of the "bad guys?"

This is a small taste of the world of vulnerability management, the many technologies that drive it and the social intricacies that will continue to mold it. Everyone is talking about security until we are all blue in the face. At the end of the day, I fear too many people are doing just that, talking. Security in my mind is still not a true priority for organizations. Organizations will all admit that security is the most important thing to their business, but when push comes to shove and business decisions are made, security still remains riding in the backseat of a broken down vehicle that is riding the information highway to nowhere.

Signed,
Marc Maiffret
Co-Founder/Chief Hacking Officer
eEye Digital Security

June 2, 2004

Marc Maiffret
Chief Hacking Officer
eEye Digital Security

Congressional Subcommittee Testimony on Security Threats to Public and Private U.S. Infrastructure

Vulnerability Management Strategies and Technology

For some time, security has been a race to create new protection mechanisms for a never-ending onslaught of vulnerabilities. Vulnerabilities are at the core of what makes systems insecure. However, the vulnerabilities that organizations face are not simply system/software vulnerabilities, but also social vulnerabilities in how people interact with technology. Until not long ago most organizations were winning the security race, because the "bad guys" were letting them. Things have changed though, attackers have become smarter, and the race is over. The "good guys" have lost, for now, and there has never been a better time to be a criminal.

One of the main reasons for the "good guys" losing this battle is due to the fact that security has always been reactionary. With the current trends in vulnerabilities, there is no time to react. It is important to emphasize the reactionary state of security to help better understand the dynamics of why we are failing.

Patches Aren't Always The Answer

If you casually look at the available studies and statistics you can easily point the blame at organizations for not patching their systems. Then again, you can also read newer studies which say patching is not enough - you cannot patch in a reasonable amount of time before new threats emerge (worms, viruses, exploits, etc.). Others say that it is not a problem of not patching or not patching fast enough, but there is an increase in "zero-day" vulnerabilities or threats that take advantage of non-public vulnerabilities which do not yet have patches. Keeping all of these dynamics in mind, you have to realize that the threat of vulnerabilities, which can be fixed through patches, is only one of a few different types of vulnerabilities that organizations face. Organizations are also vulnerable to various software/system configuration vulnerabilities, as well as social vulnerabilities.

Misconfigurations and social vulnerabilities are the most publicized types of attacks, and also the least. Virus attacks are one form of social vulnerability that is typically made very public. Viruses are able to propagate from system to system based on human interaction with software in a way that is harmful to the system the software is running on. The problem then escalates from one infected system to entire companies and groups of computer users. There are other types of vulnerabilities in software and systems that can be leveraged by attackers who take advantage of misconfiguration weaknesses in order to gain access to resources that attackers shouldn't otherwise have

access to. One recent example of this is when internal memos from the Senate Judiciary Committee were compromised. I'm sure you're all familiar with that particular instance. A solid Vulnerability Management plan will also cover the aspects of policy and compliance, user education and various other security facets beyond simple patch remediation.

Security According to Specific Needs

Vulnerability management should be at the heart of every organization's security strategy. Most organizations would love to have the single silver bullet for vulnerability management. While security companies will all claim that they offer it, there is no one solution. Instead, one of the most important aspects of creating a good vulnerability management plan is to first understand what is critical within your organization. From the private sector to the public, from financial services to health care, there are many differences in what is critical within an organization, and therefore different security requirements.

One of the first things to accept in securing a large enterprise is that the odds of being impervious to attack are against you. This is as good as a drunken road-trip to Vegas and betting your next house payment on black. There are no two ways around it; the odds that there will always be a way for a hacker to penetrate your network are against you. That is why it is important to understand what is critical within your organization and focus on those critical points first, before trying to tackle the security of your organization in its entirety. Obviously there are various levels of security a company can obtain, and with that, there are various layers of security that are required to advance to the next level. To understand what layers of security are required for your organization to reach various levels of security, you must first understand the types of threats your organization could possibly face.

Imagine for a moment that there are potentially thousands and thousands of people who live for "the thrill of the hack." From the young boy working all hours of the night to find that next vulnerable system to the next virus writer hoping to see their work made public around the world, there are many different types of computer criminals, and for the most part none of them seem to care which computers they target. Now take that image of computer "criminals" and never think of it again. Times have changed. Though some things have remained the same, the motivation and people behind computer intrusions has drastically changed.

As with any "free" and open system (computers, networks, Internet, etc.), that relies heavily on trust, the fun has to eventually come to an end. The "bad guys" have grown all too knowledgeable about the fact that technology is creating new opportunities to profit and proliferate from the same common criminal ideas that have existed for many years. This is all very evident by the investigations into various online fraud activities performed by the Federal Bureau of Investigation, many of which lead back to various countries where organized crime is able to operate more freely because of lax computer security laws and poor relations with the United States. There are other attacks, beyond simple online fraud, that are more sophisticated. Attacks that target specific companies and leverage things unique about an organization in order for an attacker to acquire whatever it is they are after. Regardless, if you want to believe the "boogeyman" stories

of organized crime or foreign nations breaking into your computer networks, the one attacker that almost all organizations have met with face-to-face is the computer worm.

A computer worm is a program that leverages a "vulnerability" (typically found in software) to replicate itself from one computer to another without requiring any human interaction. Depending on the computer worm, there is sometimes a "payload" that is included with it. Payloads can be anything from malicious code that uses thousands of worms to create a coordinated attack against a target system, or a payload could simply attempt to disrupt or destroy data on infected systems. While the idea of computer worms sounds scary, the idea is nothing new.

Computer worms have been around for some time now. However, they are becoming more and more popular and seemingly easier to produce than ever before. One of the first known records of a computer worm stems all the way back to 1988 when Robert T. Morris Jr. released the first computer worm, seemingly by accident. One interesting aspect of the first computer worm was not specifically about the worm itself but more so about the author. The father of Robert T. Morris Jr., at the time the worm was released, was none other than Robert Morris who was then the Chief Scientist of the National Security Agency (NSA). Some would later speculate whether or not Robert T. Morris Jr. came up with the concept of the computer worm on his own. While there is interesting mystique surrounding the first computer worm, we must remember one thing. The first computer worm was written over 16 years ago. We have had 16 years to think about, analyze and create solutions to guard against computer worms. So why after all of this time, are businesses constantly impacted by computer worms? More so, why are businesses still impacted by vulnerabilities?

Vulnerabilities Are Typically A Known Quantity

Vulnerabilities in software and systems are what allow computer worms to propagate in the first place. When a vulnerability is discovered, typically that vulnerability is reported to the manufacturer of the software in which the vulnerability is found. At that point, the software vendor begins to assess the risk that the vulnerability poses to its customers. In some cases, the vendor also assesses the risk of embarrassment they will endure in the media. After some time, the vendor will eventually release a security patch and security bulletin to notify its customers of the new risk and that they need to apply the relevant patch. Parallel to that, the security researchers who discovered the vulnerability will also release a security bulletin that describes the vulnerability and gives possible mitigation information that can be put in place until a patch is deployed. At this point, a vulnerability has been made public. From the patch itself, enough knowledge has been disseminated that allows attackers to create worms and exploits, or programs that can take advantage of a vulnerability to compromise computer systems running the vulnerable software. This is when security starts to fall apart in the vulnerability life cycle. The reason being, vulnerabilities are being exploited faster than organizations are able to react to them and patch their systems. Therefore, even the most security-astute organizations are still going to be impacted by worms and computer attackers.

Some people have equated the current "vulnerability lifecycle" in relation to the term OODA Loop, or Observation Orientation Decision Action Loop, which was first

coined by Col John Boyd, USAF (Ret). In relation to vulnerabilities, the idea of the OODA Loop is that if an attacker can get "inside" your OODA Loop they will have the upper hand, as organizations will not be able to properly respond to attacks and instead be left in a helpless and disoriented state. All analogous jargon aside, if exploits and worms are being released before organizations can react, organizations will continue to be impacted by the ever-growing number of threats.

Coming around full circle we know that having good vulnerability management means good security policy and compliance, user education and technologies that will allow your organization to regain control of the vulnerability lifecycle. There are many technology solutions and service providers that cover the various areas of vulnerability management. One of the first steps an organization must take is determining a trusted source to help them along their path of creating a good vulnerability management plan. Many organizations actually do have a wealth of security knowledge within them just waiting to be tapped into. An outsider's perspective can also be helpful for organizations in determining their current security stance and critical business processes.

Angles Of Vulnerability Management

When it comes to vulnerability management, there are a few basic technologies with varying levels of sophistication. Most of the technology related to vulnerability management can be separated into two functional groups: perimeter and endpoint, or host-based, security. There is, however, one technology that plays an important part in both perimeter and endpoint security - vulnerability assessment. The first place that companies typically make an investment in security is around the perimeter of their network.

Perimeter security is one of the older forms of security which for many years has been made up of two main types of security solutions: firewalls and Intrusion Detection Systems. Firewalls were created to provide access controls on how systems are allowed to communicate with one another. While firewalls worked very well for their intended purpose, they eventually were not enough to handle all the new emerging threats. Based on that line of thinking, the idea of the Intrusion Detection System (IDS) was born.

IDS created a way to monitor all network communications for various attack patterns and then create notifications based around those attack patterns. Those notifications were then interpreted by an organization's IT staff to determine whether or not a system really had been compromised. This technology is no longer a viable option as most organizations have realized that IDS requires too many personnel resources without much return on investment. From this failure and various market analysts proclaiming, "IDS is dead," there was the birth of Intrusion Prevention Systems (IPS).

IPS is the next wave of perimeter security that aims to protect organizations from both known and unknown attacks. Unlike IDS, IPS is supposed to actually stop attacks, and not just notify organizations about them. Therefore, giving an increased level of security by blocking attacks around the perimeter of your network. The problem though is that many IPS solutions are nothing more than repackaged IDS solutions that have been repurposed to "block attacks" instead of just notifying organizations about attacks.

One of the fundamental flaws of IDS/IPS systems, regardless of whether or not they are able to block attacks, is that they protect against exploits and worms which are not necessarily the core of the security problem organizations face. Again, the core of the security problem is the vulnerabilities. Since IDS/IPS systems are protecting from exploits and worms, the threats, and not vulnerabilities specifically, they fall into the same vulnerability lifecycle trap that was described earlier. Again, your security is only as good as how quickly your IDS/IPS system can be updated. You might have gained a little bit of time in the race against attackers; however. in most cases you still have not gained enough time to win the race. In general, firewalls, IDS and IPS, do have their applicable uses and every company should, at the very least, be investing in perimeter security. It should, however, be understood very clearly that perimeter security is not enough. One of the reasons why perimeter security, no matter what kind (firewall, IDS, IPS, etc.), is not enough is because the dynamic nature of threats and business processes has created a plethora of ways that attackers, worms, etc. are able to find their way inside an organization's network.

Companies who have invested heavily in perimeter security are still being affected by various security threats for a few reasons. One of the reasons is that of remote and rogue computer users. Whether it's a user traveling with a laptop on the road or logging in from home, all too often, remote users' machines are being infected with worms, or "back-doored" by attackers. Eventually those remote users bring their systems back inside the organization, at that point, bypassing any perimeter security that is in place. Remote and rogue users are not the only ways perimeter security is being unknowingly bypassed these days. Other breaches in perimeter security are commonplace in relation to business processes that require two organizations to communicate between one another, often times from within each organization's perimeter. From these various deficiencies in perimeter security came the idea of endpoint security solutions.

Endpoint Security

Endpoint security will receive a great deal of attention over the next few years. This is because endpoint security solutions are providing security at the closest point to the digital assets that organizations are trying to protect. There are many types of endpoint security solutions and many of them are similar, if not identical, to some perimeter security solutions. Patch management solutions are also a part of endpoint security and are growing in popularity.

No one can deny that one of the most crucial things an organization needs to be doing for security is installing the latest security patches. There are many adequate solutions on the market today that allow for organizations to deploy patches across their environment with relative ease. When looking at patch management solutions, organizations need to be careful about the scalability of certain patch management solutions. While a patch management solution might seem like a great idea in concept or in a lab, many patch management systems start to break down and have problems when they are used on a network of any sort of large scale. Another deficiency in most patch management solutions is that their management capabilities, beyond even scalability,

have not been built with large organizations in mind. Patch management and remediation is not as simple as clicking a button and blasting a patch out to all the systems that need it, although that's how most patch management solutions work. Patch management is very much process-related, and the process of deploying patches changes depending on each organization. Even a scalable and process-oriented patch management solution is not going to be enough to protect your organization. Again, the current vulnerability lifecycle does not allow organizations enough time to patch before a new threat emerges. That does not mean you should not be looking into patch management or patching your systems...just don't bet the farm on it.

One security technology that has been pioneered recently has been that of Endpoint Vulnerability Protection. Endpoint Vulnerability Protection works by being able to understand the vulnerabilities that are used by exploits, worms and attackers. By truly protecting systems from vulnerabilities and not threats, EVP systems are able to protect systems automatically from new threats, before they arise. That is to say that when a vulnerability is released, an EVP system is then able to specifically protect a system from that vulnerability. So no matter what new threats, worms or otherwise, are released, your systems will already be protected ahead of time; therefore, giving you the advantage in the vulnerability lifecycle. This then allows you to deploy patches throughout your organization when it makes sense for your business. Your systems remain protected even without patches installed.

While endpoint security in some ways sounds like the silver bullet to security you must keep a few things in mind. First, there are many different types of endpoint systems that organizations need to protect: Windows, Linux, Apple, Unix, routers, and various other devices. Most endpoint security solutions do not offer support for all of these different platforms, and some platforms are simply impossible to create endpoint security solutions for, as they are proprietary. Also, endpoint security solutions are only going to protect systems that organizations know about and systems on which they can install endpoint agents. There is still the threat of rogue machines, machines that cant run the endpoint agent software, and various other instances where endpoint security is not applicable. These are just a few of the reasons that some of the largest organizations in the world rely on one of the oldest type of vulnerability management tools ever created: vulnerability assessment.

Vulnerability assessment is a solution that can provide organizations with a clear view of their current security stance, whether it is perimeter security, endpoint security, rogue devices, or security policy compliance. Vulnerability assessment allows you to view the security of your network from all angles and create a real-world view of how your organization is doing in terms of its risk to malicious attackers. Years ago, Vulnerability Assessment (VA) was mostly thought of as a quick-use security-consulting tool, and for the most part it was. Over time, VA solutions have evolved into enterprise-class security solutions that provide companies the real-time information they need to properly assess their security posture when new threats are discovered. Beyond that, VA solutions have evolved into more process-centric solutions that allow organizations to track vulnerabilities from their initial discovery all the way through their remediation. This allows organizations to have a better understanding of the types of vulnerabilities

they are facing, as well as management of the personnel and resources that are required to ascertain various levels of security.

One of the last technological building blocks of vulnerability management is a solution to manage the many processes that make up vulnerability management. Whether it's your perimeter security, endpoint intrusion prevention, or patch remediation, the various solutions for vulnerability management alone are not enough. Having the various tools to perform vulnerability management does not necessarily mean you have created the business processes to verify that everything is in compliance to your set standard. The end-to-end vulnerability management plan should include a solution to manage the process as a whole. Simply having vulnerability assessment, firewall, patch remediation tools, etc. is not enough. You need to have a process to track your organization's progress and verify that you are at some level of compliance relative to your business goals. Organizations must also remember that one of the most important natural resources and backbones of security and vulnerability management is the security researcher.

Security researchers come in many forms from the hobbyists staying up all hours of the night finding security bugs for fun to the paid employee working for a security companying researching new vulnerabilities. No matter what type of security researcher, security researchers are critical assets in helping organizations gain a level of security. That is not to say every organization must have their own security researchers on staff, but organizations must remember that by wanting their systems to be secure, they are in part joining a security community made up of all types of people. Organizations must be wise in knowing what people and movements/ideas they should support. There are many battles that are waged between big business and the security researcher. The majority of time "big business" is the very companies who are writing insecure software and putting organizations/customers at risk, who would rather security researchers went silent. If no one talked about the problem, then there wouldn't be a problem.

Thinking Like A Criminal, For Greater Security

Looking to the past we can find instances where battles were staged. Organizations, researchers, companies, and even government, all took sides on debates about security. Had some of these debates gone truly sour, we would have seen a rippled effect that would have caused a giant set back to the security of organizations today. So what was one of these historical turning points where community decisions on security could have caused things to go horribly wrong? The birth of vulnerability assessment. One of the very first vulnerability assessment tools ever created was SATAN. When SATAN (System Administrators Tool for Analyzing Networks) was first created many organizations and institutions went into a bit of a panic. Some people got the idea in their head that the creation and public release of vulnerability assessment tools would allow for the "bad guys" to use the tools against organizations and therefore help the "bad guys" in their efforts to break into systems. The creators of the tool argued that the tool was needed by the "good guys" in order to be able to identify all the ways that the "bad guys" could break into systems and have information on how to fix those insecurities. The creators believed so strongly that they were doing what was right for security that at least one of the creators put their professional career at risk. A long time

before SATAN was created, "bad guys" had been using these types of tools to break into computer networks, but the "good guys" were never clued in to have the same tools as the "bad guys." The idea of thinking like a criminal, to stop a criminal seemed a hard pill to swallow at the time. If you look at present day security you will see that vulnerability assessment tools are very common-place within organizations and are widely accepted as being one of the greatest network security tools. This is just one example that hopefully illustrates the need for organizations to stay in touch with security researchers, their ideas and their motivations. Where would organizations be now if vulnerability assessment tools had been outlawed? Where will organizations be tomorrow if free thinking and publication of vulnerability research and exploits were outlawed? Shouldn't we be more concerned, first and foremost, with the accountability of companies creating the insecure software? When the battle is waged between researchers and software vendors for accountability on both parties' parts (researches for their information and software vendors for their insecure software) where will your organization stand? Or will you not be informed enough to lend a hand in making sure computer security keeps progressing ahead of the "bad guys?"

This is a small taste of the world of vulnerability management, the many technologies that drive it and the social intricacies that will continue to mold it. Everyone is talking about security until we are all blue in the face. At the end of the day, I fear too many people are doing just that, talking. Security in my mind is still not a true priority for organizations. Organizations will all admit that security is the most important thing to their business, but when push comes to shove and business decisions are made, security still remains riding in the backseat of a broken down vehicle that is riding the information highway to nowhere.

Signed,
Marc Maiffret
Co-Founder/Chief Hacking Officer
eEye Digital Security

Mr. PUTNAM. Thank you, Mr. Maiffret.

Our next and final witness for this panel is Steve Solomon, chief executive officer of Citadel Security Software since its formation in December 1996 and as president and CEO of CT Holdings since May 1997. Mr. Solomon spent 8 years in the security software industry.

Citadel Security Software creates and provides full life cycle vulnerability management solutions that protect information technology infrastructures. Mr. Solomon is a board member of the Cyber Security Industry Alliance and served as the chairman of the Committee on Computer Privacy and Data Security Standards, a private sector initiative that followed the work of the Privacy Roundtable led by U.S. Senator John Cornyn, formerly attorney general of Texas.

Welcome to the subcommittee. You are recognized for your testimony for 5 minutes.

Mr. SOLOMON. Good afternoon, Mr. Chairman and members of the subcommittee. I want to thank you for the opportunity to appear today to discuss vulnerability management strategies and technology.

Before I start, I want to applaud the committee for having the commitment and vision to help our Nation's drive awareness and direction to this ever growing security threat facing our critical IT infrastructure.

Today's organizations face exponential growth in the number of vulnerabilities and the speed at which the attacks are introduced. At a recent DOD Information Assurance Conference, it was predicted by the year 2010, we will face nearly 400,000 new vulnerabilities per year which equates to roughly 8,000 vulnerabilities per week or one new vulnerability every 5 minutes.

By successfully exploiting one vulnerability, organizations are exposed to potentially tens of millions of dollars in economic damage and successful attack on our Nation's critical infrastructure could result in life threatening events, jeopardize our national security and impact our way of life.

By the year 2010, it is estimated there will be half a billion users on the Internet. In a society open like ours, our complex organizations, remote employees and open access to systems, we are targets for individuals and organizations that want to attack us. We cannot let September 11 repeat itself in cyber space.

To be prepared for this onslaught, we must continue to expand the foundation that the committee has initiated. Expansion must include the need for sound vulnerability management processes, supporting technology and the necessary legislation to ensure our Nation's critical IT infrastructure is protected. We have seen the sophistication and speed of the attacks mature to where the existing security measures such as firewalls and a virus are not enough to stop these attacks. By fixing known vulnerabilities, we can proactively eliminate cyber threats, reduce risk and deliver a more secure IT infrastructure.

Organizations must take a proactive stance and implement a full life cycle vulnerability management capability. Success requires new processes, automated technology to support these processes and management's commitment to drive the needed change.

In the public sector, FISMA is helping to drive initiative in the awareness for improved cyber security. However, interpretation has not been consistent throughout all agencies resulting in inconsistencies and actions to address these problems. However, there are excellent examples of organizations that have already implemented proactive vulnerability management processes such as the Department of Veterans Affairs and National Finance. In addition, other agencies such as FAA, the DOT, IRS and Department of Defense have all started taking proactive steps to address the need for full life cycle vulnerability management.

For most of corporate America, the process is broken or fragmented across different groups using point tools and manual techniques. There are some industries ahead of others primarily driven by the mandates of Sarbanes-Oxley, GOB and HIPPA which are driving awareness and need for more proactive uses. However, the interpretation of these mandates and the required action to comply are too broad resulting in ineffective results leading to continued attacks and exposure on a daily basis.

Compounding the problem across both the public and private sector is the increased number of remote users who return to the enterprise networks with compromised environments results in continued introduction of malicious attacks after remediation actions have taken place. Organizations have implemented some form of patch management tool have a false sense of security. On average, only 30 percent of an organization's verified vulnerability relates to patching, leaving the network exposed to the remaining 70 percent of the problem which are more dangerous and easily exploited. These products do not address the problem of full life cycle vulnerability management and effectively become part of the problem.

To successfully deliver a full life cycle vulnerability management process, automation is a necessity. The ability for multiple security and IT operations disciplines to work together requires technology that provides an integrated platform by which to manage the process. Leveraging automation will shift organizations from reactionary to a proactive vulnerability capability.

Technology is available today to deliver the flexibility of automated vulnerability management. A key requirement is solutions that provide seamless integration across the assessment and remediation steps of the process. Full function remediation solutions must address all types of IT vulnerabilities and provide a mechanism to report on the progress from the assessment to mitigation to the ongoing compliance. In order to streamline the process, solutions must provide a comprehensive library of remediation actions identified to fix the vulnerabilities with the ability to rapidly deploy the remediation actions across the network on a consistent, repeatable process.

As new vulnerabilities are discovered on a daily basis, there must be a mechanism to continually deliver new intelligence and remediation actions that are tested. To mitigate the impact to remote users, solutions must provide capability to both quarantine and remediate devices upon the network connection.

The commercial software industry must be involved in providing solutions. NIAP common criteria certification is an excellent step in the endeavor, yet there is no enforcement across the public sector

to purchase products that are common criteria certified. We recommend the Government lead the way in requiring software solutions be certified and common criteria at AL3 or above before they can be procured for implementation.

To further reduce the risk, we must address the concern of offshore development. A major portion of the software development today occurs offshore. We must ask for additional controls to ensure software development overseas is secure. Software development organizations should be required to have all overseas development of software examined for malicious capabilities embedded in the code. Industry and Government must work together to develop some form of standard to review the process to address the growing threat.

A few months ago many leaders from the cyber security industry came together to form an important alliance. The Cyber Security Industry Alliance represents the latest commitment from cyber security industry to positively enhance information security. I am proud to say Citadel serves as a board member on the committee. The mission of CSI is to enhance cyber security through public policy initiative, public sector partnership and corporate outreach, academic programs and alliance behind emerging industry technologies.

In conclusion, the vulnerability management is a core security requirement. By successfully implementing a proactive, automated approach, organizations can reduce the risk and mitigate their exposure to cyber threats. Industry and academia must work together closely with Government to drive awareness, education and provide direction across public and private sectors with national security efforts.

I thank the committee for the opportunity to testify.

[The prepared statement of Mr. Solomon follows:]

The U.S. House of Representatives Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on
Information Security – Vulnerability Management Strategies and Technology

June 2, 2004

Statement Submitted for the Record
By
Steven B. Solomon, Chief Executive Officer,
Citadel Security Software Inc.

Good afternoon Mr. Chairman and members of the subcommittee.

I want to thank you for the opportunity to appear today to discuss vulnerability management strategies and technology. Before I start, I want to applaud this committee for having the commitment and vision to help our nation drive awareness and direction to the ever growing security threats facing our critical IT infrastructure.

Introduction

Today organizations face exponential growth in the number of vulnerabilities and the speed at which attacks are being introduced. At a recent DoD Information Assurance conference it was predicted that by the year 2010 we will be faced with 400,000 new vulnerabilities per year. That equates to roughly 8,000 vulnerabilities per week or one new vulnerability every five minutes. By successfully exploiting one vulnerability organizations are exposed to potentially tens of millions of dollars in economic damage. A successful attack on our nation's critical infrastructure could result in life-threatening events, jeopardize our national security and impact our way of life.

By 2010, it is estimated that there will be half a billion users on the Internet. In an open society likes ours, with disperse and complex organizations, remote employees and open access to systems, we are targets for individuals and organizations that want to attack us. We can't let 9/11 repeat itself in cyber space.

To be prepared for this onslaught we must continue to expand the foundation that this committee has initiated. Expansion must include the need for sound vulnerability management processes, supporting technology, and the necessary legislation to ensure our nation's critical IT infrastructure is protected.

Nature of the Problem

We have seen the sophistication and speed of cyber threats mature to where existing security measures such as firewalls and anti-virus software are not enough to stop these attacks. By fixing known vulnerabilities we can proactively eliminate cyber threats,

reduce risk, and deliver a more secure IT infrastructure. Organizations must take a proactive stance and implement a full lifecycle vulnerability management capability. Success requires new processes, automated technology to support those processes, and management commitment to drive the needed change.

In the public sector FISMA is helping drive initiatives and awareness for improved cyber security. We believe a key aspect of FISMA is to ensure all agencies comply with assessing, remediating and reporting on compliance; however, interpretation has not been consistent through out all agencies resulting in inconsistent actions to address the problem. However, there are some excellent examples of organizations that are taking a proactive stance and making solid progress in this battle. For example, the VA's OCIS Director, Bruce Brody, had the vision and recognized the challenge around vulnerability management. Mr. Brody has directed an organization-wide program mandating a comprehensive vulnerability management process and implementation of supporting technologies to proactively remove vulnerabilities such as unsecured accounts, mis-configurations, unnecessary services, backdoors, and software defects. Other government agencies, such as the FAA, IRS, and Department of Defense are taking proactive steps to start addressing the need for a full life cycle vulnerability management process. The DoD's information assurance vulnerability management (IAVM) initiative is working to address the problem head on. For example, the Army Chief Information Officer's information assurance efforts are aligned with DoD and together they are working to deliver effective initiatives and workable solutions. We are seeing other key branches of the armed forces coming together to address the problem in similar fashion.

In the private sector we have seen limited progress in addressing these issues. Attacks and compromises to networks occur every day. Living in a false sense of security by occasionally applying patches, not doing proper vulnerability assessments, and treating the vulnerability management problem in a reactive mode is the result of a lack of process. For most of corporate America, the process is broken and fragmented across different groups using point tools and manual techniques. There are some industries ahead of others primarily driven by mandates to drive awareness and the need to be more proactive. For example, GLB in the financial sector, HIPPA in the health care sector and Sarbanes Oxley for public companies. However, the interpretation of these mandates and the required actions to comply are too broad resulting in ineffective results leading to continuous attacks and exposure on a daily basis.

Compounding the problem across both the public and private sector is the increased number of remote users who have the ability to connect to multiple networks resulting in compromised environments. When the remote worker returns to the enterprise network their compromised environment results in the continual introduction of malicious attacks after remediation actions have taken place.

Organizations that have implemented some form of patch management tool have a false sense of security. On average only 30% of an organization's verified vulnerabilities relate to patching, leaving their networks exposed to the remaining 70% of the problem which are more dangerous and easily exploited. These products do not leverage

independent vulnerability assessment data to drive the remediation process, provide compliance reporting, or have the ability to establish security policy and enforce a secure state. Further, these products do not address the problem of full life cycle vulnerability management and effectively become part of the problem.

Addressing the Challenge

Defining the vulnerability management process has several key elements. First, the process has to be enforceable across multiple disciplines and accountable to the highest levels of the organization. In addition, the process must be pragmatic and scalable to meet the needs of large organizations dispersed across global boundaries. Once the process is defined, necessary technologies have to be employed to automate. Without automation it is impossible to address the growing number of vulnerabilities in a timely, cost effective manner. Lastly, the appropriate legislation must be established including directives to specifically address the need for sound vulnerability management practices.

The challenge for many organizations across both the public and private sectors is funding. Corporations must better understand the exposure to and liability of cyber attacks as well as the resulting benefits of implementing the correct process and technologies in their environment. Hackers and terrorists are moving faster every day and implementation of these strategies must move in sync. We must invest now to establish a base line and protect the economic future of the corporation, its shareholders, and our national security.

A Full Lifecycle Vulnerability Management Process Defined

A full lifecycle vulnerability management process provides a proactive approach to eliminating IT vulnerabilities and ensuring they do not reoccur. The first step is to identify and categorize all IT assets. The second step is to assess the environment and identify vulnerabilities. The third step requires a thorough review of each vulnerability and assessment of its criticality. The fourth step involves defining the appropriate fix and applying the fix consistently across the enterprise. The fifth, and last step, requires the establishment of security policy which defines the secure state and the ongoing enforcement of that secure state.

Automating the Full Lifecycle Vulnerability Management Process

To successfully deliver a full lifecycle vulnerability management process, automation is a necessity. The ability for multiple security and IT operation disciplines to work together requires technology that provides an integrated platform from which to manage the process. Leveraging automation will shift organizations from a reactionary to a proactive vulnerability management capability.

Technology is available today to deliver a flexible automated vulnerability management capability. A key requirement are solutions that provide seamless integration across the assessment and remediation steps of the process. Full function remediation solutions must address all types of IT vulnerabilities and provide a mechanism to: report on progress from assessment, to mitigation, to on going compliance. In order to stream line the process, solutions must provide a comprehensive library of remediation actions to

identify and fix each vulnerability along with the ability to rapidly deploy remediation actions across the network in a consistent repeatable manner. As new vulnerabilities are discovered on a daily basis there must be a mechanism to continually deliver new intelligence and remediation actions. To mitigate the impact of remote users, solutions must provide the capability to both quarantine and remediate devices upon network connection.

The commercial software industry must be involved in providing quality solutions. Industry is cooperating and working to assure success. NIAP Common Criteria certification is an excellent step in this endeavor. Yet there is no enforcement across the public sector to purchase products that have received CC certification. Agencies are purchasing and deploying solutions that are not certified, or are in the process of applying for certification with no assurances of completing the process resulting in diminished value of the certification program. We recommend the government lead the way in requiring software solutions be certified to Common Criteria EAL3 or above before they can be procured and implemented.

To further reduce risk we must address a concern with offshore development. A major portion of the software developed today occurs offshore. We must add additional controls to insure software developed overseas is secure. Software development organizations should be required to have all overseas developed software examined for malicious capabilities embedded in the code. Industry and government must work together to develop some form of standard or review process to address this growing threat.

Mr. Chairman, a few months ago many leaders in the cyber security arena came together to form an important alliance. The Cyber Security Industry Alliance or CSIA represents the latest commitment from the cyber security industry to positively enhance information security. I am proud to say that Citadel serves on the board of CSIA.

The mission of CSIA is to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. At the heart of that mission, Mr. Chairman, is the full support for your efforts and those in the private sector to make information security a core corporate governance issue at the C and boardroom levels.

Conclusion

In conclusion Mr. Chairman, vulnerability management is a core security requirement. By successfully implementing a proactive, automated approach organizations can reduce risk and minimize their exposure to cyber threats. Industry and academia must work closely with government to drive awareness, education, and provide direction across the public and private sectors to this national security problem.

The Evolution of Patch Management to Full Lifecycle Vulnerability Management
by Carl Banzhof, CTO, Citadel Security Software

One of the most compelling figures I've seen regarding the state of IT security comes from British computer security firm, Mi2G, which puts the economic impact of Internet-based intrusions for February 2004, just February, at an estimated $68 to $83 billion worldwide. With CERT®/CC reporting roughly 70 to 80 new IT system and network vulnerabilities per week and over 95% of the successful cyber attacks resulting from "known vulnerabilities or configuration errors where countermeasures were available" it is no wonder that most companies today are looking for ways to remove these flaws before they can be exploited and cause, at a minimum, disruption in service and in many cases, result in loss of sensitive data, economic damage, and tarnished reputation.

Today's enterprise is charged with the serious responsibility of weighing and managing security risk. It's the age-old formula that equates risk with *vulnerability x assets x occurrence rate*. Admittedly, most organizations do not have the luxury to change the IT assets they have, nor can they possibly control the occurrence rate of sabotage attempts. However, they *can* control vulnerabilities - what's going on inside their organization. With the plague of vulnerabilities that infest today's IT systems and networks – add to this the new job requirement placing senior level officers in charge of managing and mitigating risks to meet corporate governance standards, audits and regulatory mandates – it's no wonder that traditional patch management is no longer a viable option for comprehensive security practice.

Patch management is a reactive response to external risks and from a security perspective is inadequate because of the following key limitations:

Five Classes of Vulnerabilities

- Unsecured Accounts
  - user account left dormant or possessing unnecessary privileges, i.e. Null Password, Admin no PW, no PW expiration…
- Unnecessary Services
  - default applications or operating systems such as Telnet, Remote Access, Remote Exe…
- Backdoors
  - programs that allow remote access and computer control such as NETBUS, BACKORIFICE, SUBSEVEN…
- Mis-configurations
  - system and application vulnerabilities that are resolvable, i.e. NetBIOS null sessions...
- Software Defects
  - the most discussed of vulnerabilities such as Hot-fixes, Patches…

1. The reactive "attack & patch" approach consumes unplanned and intensive levels of labor, requires long cycles, provides limited control at best, and actually increases the probability of undoing past securing efforts.
2. Patch management only addresses software defects which represent 20 to 30 percent of the critical system and network vulnerabilities found in most IT environments. Apart from exploitable software defects, there are four other classes of vulnerabilities that constitute the remaining 70 - 80 percent of critical vulnerabilities related to IT security. These include *unsecured accounts, backdoors, unnecessary services* and *mis-configurations*.
3. Patch management tools do not provide integration with commercially available vulnerability assessment tools – most patch management solutions have built-in

system scanners to identify needed software patches. Without this integration there is no systematic way to comprehensively identify and organize vulnerabilities into meaningful data that operational staff can act on.

From an operational standpoint patch management once seemed the best available option for addressing vulnerabilities. However, organizations today are realizing that patch management only addresses a very small piece of the vulnerability puzzle and is not enough to address their security concerns. The larger chunk of the equation involves a security process that in and of itself, spans multiple groups across an enterprise. I'm talking about your security team responsible for identifying and assessing vulnerabilities as well as your IT operations team, consisting of both network and systems administrators who are responsible for developing, testing, and deploying fixes for discovered vulnerabilities. For most companies this process is mostly manual resulting in a broken process that will not deliver the level of security, compliance, and confidence needed.

I believe the only way to improve a company's security posture and reduce risk is to automate as many processes as possible that are involved in identifying and resolving vulnerabilities. Enter *enterprise vulnerability management*, a full life cycle approach to take security efforts beyond patch management to a more proactive and holistic approach of asset classification, vulnerability identification and mitigation, and policy monitoring and enforcement.

Vulnerability management works on the basic premise that by removing the real problem – the vulnerability itself – you will minimize the number of threat occurrences to which your company is exposed, thus reducing overall risk. The following represents a best practices outline that eliminates system and network flaws through end-to-end vulnerability management across all 5 classes of vulnerabilities, ensuring the highest level of security with the least amount of interruption.

Best practices for closed loop vulnerability management

1. **Identify/Discover Systems & Devices** – inventory what aspects of your IT infrastructure – hardware, operating systems, applications and other technologies or services – are potentially the most vulnerable.
2. **Vulnerability Scanning** - proactively monitor and identify vulnerabilities specific to your environment. This step will allow for decisions regarding proactive and reactive steps necessary in order to remediate vulnerabilities.
3. **Vulnerability Review** - assess the exposure or liabilities caused by vulnerabilities for each of your assets – prioritize those that will cause the most risk to the business if exploited.
4. **Vulnerability Remediation** – counteract vulnerabilities by defining remediation actions and applying those actions through scheduled, automated end-to-end remediation.
5. **Ongoing Management** – close the loop on the vulnerabilities through policy definition and compliance checking.

The absence of an enterprise vulnerability management process creates a high-risk environment that is exposed to both internal and external security threats which can result in serious operational and financial consequences. Most security breaches could have been avoided if the proper vulnerability assessment and remediation actions had been enforced. Security attacks will only increase in frequency, degree and complexity, making vulnerability management a key IT priority.

The best advice I have for reducing today's security threats is to go beyond patch management by implementing a full lifecycle vulnerability management process and supporting software technologies to deliver an integrated approach across the different groups responsible for security processes – and automate as many steps as possible.

General Requirement for an Automated Vulnerability Remediation Solution

- Ease of use – product shall be easy to use and install.
- Interoperability with multiple security scanners – product shall integrate with multiple leading scanners on the market such as Harris STAT Scanner, ISS Internet Scanner, ISS System Scanner, Microsoft MBSA, Nessus, FoundStone, eEye Retina, and others. This will allow support of the AVR security lifecycle process of scanning, remediation and maintaining compliance with security policy.
- Vulnerability Aggregation – product shall aggregate data from multiple scanners to provide a true assessment of a security posture and expedite the vulnerability review process.
- Vulnerability analysis – product shall allow the user to review vulnerabilities and approve or disapprove for remediation
- Remediation Policy Enforcement – The product shall provide the capability to designate selected remediations at varying enforcement levels from Mandatory (required) to Forbidden (acceptable risk) which provides remediation enforcement from a centralized policy driven interface.
- Remediation – product shall remediate clients for all approved remediations for all five classes of vulnerabilities:
    - Accounts – Accounts with no PW, no PW expiration, known vendor supplied PW
    - Unnecessary Services – shutdown Telnet, KaZaa, other P2P, rsh, echo, etc.
    - Backdoors – remove backdoor programs such as MyDoom.A, W32.Beagle.I@mm, NETBUS, BACKORIFICE, SUBSEVEN, etc.
    - Mis-Configurations – correct configurations for NetBIOS shares, Anonymous FTP world read/write, hosts.equiv, etc.
    - Patches – patch buffer overruns, RPC-DCOM, SQL Injection, etc.
- Compliance Checking – product shall provide the capability to check compliancy against approved remediations.
- NIAP Common Criteria Certified to EAL3 - EAL3 provides a higher level of assurance that is required for IAVM tools. The IAVM product shall be developed to meet stringent security requirements. A vulnerability assessment of the product is also performed to meet EAL3.
- CVE Compliance – product shall be CVE compliant.
- Encrypted communications – product shall provide encrypted communications among distributed components.
- IAVM Support – product shall support any IAVA database source to respond and maintain compliance with IAVA bulletins.
- Device Support – product shall support multiple platforms including Windows, Linux and major Unix OS such as Solaris, AIX and HP-UX.
- Group Management – product shall allow grouping of devices to manage remediation and control access to devices.
- Roll-Based Access Control – product shall allow groups of devices to be managed based on roles to establish separation of roles different tasks such as vulnerability review and remediation of devices.
- Network Protection – product shall prevent disconnected / remote users from connecting to the internal protected network if they are not compliant with their required remediation. It shall also require the required remediation to be performed.
- Reporting – product shall provide multiple reports to determine remediation success and trending.
- Distributed Patch Repository - The product shall provide the capability to load balance and distribute the bandwidth associated for patch distribution to repositories installed in various strategic locations.
- Custom remedies - The product shall allow users the ability to customize any delivered remediation actions to fit a particular purpose as well as create new remediation actions from scratch.

- Microsoft Windows 2000 / 2003 Server Certified. The product shall be certified by Microsoft to run on Windows 2000 or 2003 Server editions.
- Multiple Sources of New Vulnerability Reporting – vendor shall monitor multiple sources of vulnerability reporting and quickly provide remediation to latest discovered vulnerabilities
- Security Team Monitoring Vulnerabilities and Exploits 24x7 – vendor shall have a dedicated team of security experts to monitor for new vulnerabilities and exploits 24x7
- Remedy library. - The product shall be delivered with tested and validated remediation actions for all platforms that the product supports. The library should be supported by a dedicated team of security professionals within the organization.
- Automatic Update Service – product shall securely provide up-to-date remedies for newly identified vulnerabilities on a regular basis.
- Embedded Security Center Portal – product shall have an embedded security portal that will provide quick access to security and product related information
- Remediate by Policy – product shall accurately deploy remediation based on security requirements without the need of a SCAN
- Application Remediation – product shall support remediation of applications like MS SQL, MS Exchange, IIS, MS Office, IE and others.
- Automated agent distribution – product shall support automated agent distribution to individual devices and groups of devices to facilitate ease of deployment.
- Remediation Templates – product shall support remediation groups to be used as templates to represent a specific security policy. Multiple templates may be applied to devices and templates should be exportable and sharable.
- Support Standard Hardening Policy – product shall deploy and maintain compliance for industry standard hardening policies, such as CIS Gold Standard, MS Hardening Guides, NSA Guides (STIG, etc.).
- Customization of Vulnerabilities and Remediations - Allows users to easily customize existing vulnerabilities and remediations.
- Patch Interdependency – the product shall calculate patch interdependencies and automatically deploy the patches needed based on the installed products and drivers.
- Patch Uninstall – product shall report if a patch was uninstalled or needs to be reapplied.
- Web-Based UI – product shall have a web-based user interface, the tool goes where the administrator goes

Mr. PUTNAM. Thank you, Mr. Solomon.

Ms. Beinhorn, Mr. Culp, the other three panelists have had some interesting observations to make about the software development community. Mr. Rosenthal supported that you do your fair share, Mr. Solomon called for expanded use of common criteria and expanded software assurance programs, particularly as we look at the offshore activity that is taking place. How do you respond to that? Mr. Culp first.

Mr. CULP. We are supporters of the common criteria process. Windows 2000 has been certified. To a certain extent the valid concern about offshoring misses the point. It is not where the software is developed, it is how it is developed. Software built within the United States can be just as vulnerable as software built someplace else. What is important is not where it is built but that it is built with a solid, sound development process, that provides for independent review within the developing organization, that provides for thorough testing and that is mindful and protective against opportunities to try to insert malicious code.

With that said, the vast majority of Microsoft software, including all of our Windows products, are built in the United States in Redmond but the overall concern about offshoring I think might be more properly redirected to be concerned about oversight of the software in a tight development process.

Mr. PUTNAM. Ms. Beinhorn.

Ms. BEINHORN. At Juniper, again we take the software issue extremely seriously. We also embrace the common criteria certification process as well as the FIPPS process with an eye toward the prevention up front. You might recall Donna Meyerriecks' comments earlier today about the development process and how important it is to look at these things prior to silicon. So we take it in a very logical sort of stepped process at Juniper. All of the elements of the security that are embedded in our products are scrutinized by a team of professionals and put through a rather rigorous testing scenario against all known vulnerabilities at that time. So we fully embrace the formal process and the certification process and I agree actually with my colleague that tighter controls on those processes is certainly in the best interest of the Internet and cyber security.

To the point of offshore software, the majority of our software development is all done here but I also concur that it really doesn't matter where software is developed. I think again it is a process that requires very tight controls and very intense scrutiny.

Mr. PUTNAM. How many lines of code are we talking about reviewing to find the couple of lines that are malicious? If you are going to take it up a notch, bake in security, you are concerned about the offshore influence, what type of task are we talking about to find something someone slips in?

Mr. CULP. Well, it is a large task. All modern operating systems are in the tens of millions of lines of code order of magnitude. Trying to go through a completed code base and review it for something that somebody may have surreptitiously slipped in is very difficult and that is why it is so important to take a multilayered approach to vetting the software. You vet the individual modules as they are built, you vet the designs as they are developed, you

can vet the fidelity of the development against the design and then as you get further along in the development, you begin to bring in folks who maybe haven't seen the software before but who are experts in code level review.

One of the reasons that we participate in common criteria is because we want that external review. We bring the best minds we can to bear on writing the software but we know at the end of the day, we are human too and may make a mistake. So we want very much to include those independent, third party experts and give them an opportunity to review the product at a source code level and bring their expertise to bear to make sure we have done everything right.

Mr. PUTNAM. Mr. Maiffret, what are your thoughts on that?

Mr. MAIFFRET. I think in general, I agree it is not necessarily where the software is developed because it could just as easily be in the United States and somebody here on some sort of visa or is in the process of being sponsored. As far as being able to find bugs in software that were maliciously put there, in some cases it is almost an impossible task because as it stands right now, we still haven't even come to the point where we can automatically find all known security bugs within software. Because we can't do that, we are not going to be able to find people that are mistakenly putting bugs in there on purpose. Really, it is not a matter of can you find them and what not.

Mr. PUTNAM. If it is an impossible task, what do we do?

Mr. MAIFFRET. To take it back a level, to say it is an impossible task and at the same time say you are never going to have 100 percent security in an application, that it is an impossible task to identify all known vulnerabilities in applications, so I think we need to look at security in different ways. It is not about finding every single vulnerability that you can but about having outer safeguards around the actual components that you are trying to protect.

A real world example that is great is if you take the DIS and NSA guidelines and the STG documents, there is plenty of configuration information in there that had computers actually been set up to comply with all those configurations options, there are numerous worms that actually wouldn't have been able to infect or do anything to those computers even if they weren't patched. A lot of times there are things like that you can do that more broadly protect systems. There are also other efforts you can do which actually Microsoft is one of the leaders in one of the common types of vulnerabilities, buffer overflows and Microsoft is working with a lot of the processor community to more generically be able to protect from those kinds of attacks knowing that you are not going to be able to discover all of them within the code.

Mr. PUTNAM. Mr. Solomon.

Mr. SOLOMON. On that subject, the offshore concerns were raised with us because it is easy and cheap and maybe my colleagues on this panel have processes in place, a lot of companies don't and the process is very simple for people to call up and get something done very quick and very cheaply and there are no controls on what is coming back in. It is simply saying we don't know what we don't know today. As you said, how many vulnerabilities would be in

how many lines of code. I was at a recent conference with the Department of Defense and they estimate by the year 2010 for every 7–10 lines of code, there would be one new vulnerability. Try to find it. Once again, we have to take a proactive approach to this instead of reactionary. We have to develop a baseline, we are developing STGs and the right performance but what we are doing today in the manual process is broken because we can't keep up with the speed of the vulnerabilities unless we have a process for fixing it. Fixing everything as we talked about earlier, patching is not enough. Doing it consistently in a repeatable process, it becomes a core process of our information infrastructure.

Mr. PUTNAM. Mr. Rosenthal, it is costing your industry $1 billion a year. What are your thoughts?

Mr. ROSENTHAL. I would agree with the panelists with respect to how code is written, how code is developed. I think there is a notion of a higher duty of care, not just in the software development process but in how the software is actually deployed and used in the environment. So the same software can be deployed in my home office, on my home computer. The implications of vulnerability being exploited there has very little impact on the Nation's infrastructure. That same software product deployed in a critical infrastructure like a financial services firm, an exploitation of a vulnerability can be extremely damaging to the financial services firm as well as the critical infrastructure of the Nation.

I would tell you that I think in general the IT industry needs to understand exactly what their products are being used for, whether they be operating systems or accounting systems. They are not just products that get deployed in an environment identically. Changes are made, the way they are configured is different. In fact, the way they are managed in some cases is different. I think the industry should really spend more time understanding exactly the usefulness of these software and technology products, especially in critical infrastructure industries.

Mr. PUTNAM. How well do you think the process is today, how effectively is the private sector working with DHS to release information about vulnerabilities, to share that with the people who need to understand it before the exploits are developed? Mr. Culp and then Ms. Beinhorn.

Mr. CULP. We are actively sharing information through a number of different venues. The key point to understanding where we are coming from with respect to information sharing after the bulletin is out is that we recognize that although it may be bad publicity for Microsoft for a lot of people to know about a vulnerability they need to patch, that vulnerability isn't going to go away until people know about it and know what they need to do. So we have a very active interest in making sure that as many people know about our mistakes and what to do to correct them as possible.

I will give you one example of what we have been doing. Virtually ever Microsoft employee carries around a stack of these cards that on the one hand has a placard exhorting people to sign up for the free security updates that we send by email every time we release a security bulletin. We have several million subscribers to this free service and we send out every security bulletin that we release to that mailing list.

We are also working very closely with the CERTs, in particular U.S. CERT. We have a very close and productive relationship with DHS and believe they are vital in helping to get out the word to the U.S. computer user base but we also need to get information out to users and the rest of the world. So we actively work with CERTs in a number of different countries. As we did in the case of the Sasser worm, we contact the CERTs when the bulletin is released, we ask for their help in getting out the information to users and then when we find an attack in progress, we revisit and give them more information so everybody can stay informed.

Mr. PUTNAM. So you are generally satisfied with the process as it stands today?

Mr. CULP. I am never satisfied with the process as it stands, it can always be made much better. I would like to have to do a lot fewer of these alerts. I think that would be the best improvement we could make, to have to send out things a little less often through this channel but we do have by far the most robust communication system of anybody in the industry when it comes to reporting on security vulnerabilities.

Mr. PUTNAM. You paid a reward for someone to turn in the person who released the Sasser worm, correct?

Mr. CULP. We do have a virus rewards program. I believe the reward is paid out upon arrest and conviction. In the case of the Sasser worm, that is still being handled by law enforcement, so the program is there but the question of the Sasser worm hasn't come to finale.

Mr. PUTNAM. Is there an estimate on the damage that the Sasser worm caused?

Mr. CULP. I don't think I have seen an estimate yet and they usually vary widely depending on source.

Mr. PUTNAM. Does anyone on the panel know? Anyone have any idea? What about the charges that were leveled against the individual? What is the potential penalty for releasing the worm?

Mr. CULP. I don't know. That is a matter for German law. The individual who was arrested is in Germany and I am afraid I just not an expert in German law.

Mr. PUTNAM. Let me ask it a different way. Do you think the penalties for releasing these worms and viruses in the United States are adequate considering the damage that has been done and is capable of being done to the economy?

Mr. CULP. In general, I think I would like to see stronger enforcement and stiffer penalties. These worms are causing significant economic damage. They are requiring customers to spend serious resources to protect their enterprises and the punishment should be commensurate with the level of damage.

Mr. PUTNAM. Mr. Rosenthal, your thoughts on that same question?

Mr. ROSENTHAL. I don't know the exact penalties but I would tell you that they are not strong enough. A physical robbery of a bank, a holdup, we are limited by the amount of cash we allow tellers to have and many of those people walk rather quickly. Hackers have the ability of not just taking down a financial institution but they could knock out critical financial networks that impact our econ-

omy. So if you could tell me what the penalty was, I would tell you it needs to be doubled.

Mr. PUTNAM. Mr. Maiffret, your company has researched and found a number of vulnerabilities, often being the first one. What tools are at your disposal or at anyone's disposal to analyze code and therefore discover these vulnerabilities?

Mr. MAIFFRET. Really a lot of it comes down to the team of people we have been able to build. Obviously in-house we don't have source code to any of the software that we find vulnerabilities in so we actually look at the compiled code itself and are able to analyze it that way to find vulnerabilities. For the most part, a lot of times it is not necessarily tools that we use but just people sitting down, we have basic tools to look at a program but for the most part it is somebody actually going through how a program works and figuring out how to make it do things it shouldn't.

Mr. PUTNAM. Mr. Solomon, do you want to comment on that?

Mr. SOLOMON. Actually the discovery process internally will actually work with the CERT or scanning partners as well as the development team. A key side to that is identifying vulnerabilities in the wild as well before there are known exploits. As they are identified, we look to write the remediation fixes for them. So we have a team of engineers that actually write the remediation process so they can build a library. Today we have over 16,000 actions for cross multiple platforms for remediation so they get tested before they get applied. It is a team of engineers working with proprietary tools.

Mr. PUTNAM. Ms. Beinhorn, this spring a researcher discovered a new way to exploit a vulnerability in the transmission control protocol that would potentially have allowed substantial disruption of Internet traffic. It has serious effects on routers. What steps did your firm take when you found out about the vulnerability?

Ms. BEINHORN. That particular problem within TCP has been known for a while and companies like Juniper Networks and Cisco Systems worked along with a number of forums and the Government to resolve those issues. Yes, they were potentially very frightening but the actual truth of it is that when you architect something like TCP and it was done so many years ago, that as time evolves and systems and software evolve, different things will come up in code.

I think the resolution to this particular issue is well in hand and probably anymore detail on this topic we should contribute something outside of this forum.

Mr. PUTNAM. We talked about this in the first panel. The Government spends $60 billion a year annually in investment for IT goods and services. What can the Government do to leverage that buying power to get more security baked in?

Ms. BEINHORN. It is Juniper's opinion and strong conviction that the Government and the public and private sectors need to work more closely. I think there are lots of very legitimate and productive forums out there but with respect to the spend, which is if you distill it down for equipment, it comes in on the order of about $10-$12 billion but the development of silicon and the direction the Government wants to take need to collide and that is not something that is done overnight. It is a process that has to take into

consideration a lot of preventive measures with respect to both hardware and software.

We would like to see a more formal and closely knit relationship. The President's management agenda does call for participation by private and public entities but we work with DISA, NSA and a number of agencies. It would be better if maybe DHS was the focal point or central point for the consolidation of the go forward requirements and they were brought formally to industry for discussion and evolutionary development.

Mr. PUTNAM. Why DHS?

Ms. BEINHORN. It is a suggestion, Mr. Chairman. It seems to be the agency with, as you said, the most amount of money, so it would be logical to perhaps place the responsibility there.

Mr. PUTNAM. Mr. Culp or Ms. Beinhorn, times have changed, priorities have changed, security is a greater factor in development today than it used to be, tens of millions of computers around the world. As our security gets better with new versions of operating systems, we still will have millions of home users and small businesses and libraries and schools and everybody else that is a bit behind the curve on updating their equipment connected to the same network. As everyone agrees your security is only as good as your weakest link. How do we deal with that component of user groups even as the quality grows, the security improves, but you still have a lot of people out there using the old stuff. What do we do about that?

Mr. CULP. That is absolutely true and that is one of the biggest hurdles. We know the software we are producing today is much more capable, much more secure. It is built for the current threat and environment. We do, as you mentioned, have a very large legacy base and there are some limits to what we can do but with that said, let me give you a couple examples of what we are doing.

One thing we can do is upgrade the practices of the operators of that software. As often as not, the security of a network is dependent more on the management practices and the way it is deployed and configured than it is on the technology. So we worked very closely with some of our partners in the industry to develop deployment guides and configuration guides that will let people using the older software continue to do so effectively and securely.

We are also in some cases back porting some of the technologies I described in my written and oral testimony to previous platforms. A really good example of that is the auto update mechanism that was originally released in Windows XP and lets you automatically get patches directly from Microsoft. After we released it for Windows XP, we back ported it to Windows 2000, so the Windows 2000 users could have the benefit of that same technology. We do that whenever we can. So as much as we can, we push that better technology back to the existing legacy base and provide them with better practices to secure what they have and we try to ease the migration into the newer platforms.

Mr. PUTNAM. Ms. Beinhorn, do you want to comment on that?

Ms. BEINHORN. Actually not. I think that is less germane for Juniper than it is for Microsoft.

Mr. PUTNAM. Anyone else wish to comment on that? Mr. Solomon?

Mr. SOLOMON. Back to the older programs, a lot of it comes back to the operating system itself and configuring and setting up the system. While we can update the patches and everything else, a great example is one organization that had about 1,500 devices, did an assessment and realized they had 256,000 vulnerabilities on one network. They determined 56,000 were critical, this is a Government agency. Out of the 56,000, maybe 20 percent was related to patches and the rest were back doors, configurations, unsecure accounts, where anybody could get in and exploit that system. So it comes back to doing a total system management. It is a combination of working together. As I said earlier, a patch is not enough, you really have to focus on a complete vulnerability life cycle and close all these vulnerabilities going forward.

Mr. PUTNAM. Talk to me a bit, particularly Mr. Maiffret and Mr. Solomon, about wireless, the way everybody is going, PDAs, the home PCs that are used for remote access and laptops that are brought on-sight, you have public and private networks, these unsecured systems obviously can be corrupted and then reintroduced into the system. How do we deal with that challenge which is only growing?

Mr. SOLOMON. It is growing more and more as we get better in cleaning up our networks, then we have to worry about someone plugging back in and contaminating after a weekend. There is technology out there today that will actually quarantine a box and won't allow communication to the network before you remediate the box. So it is an automated approach, something we developed, the technology that now allows you before the communication back to the network, the box will be remediated. Today people are going to the hotel and plugging in or they come back after the weekend and utilize the device.

Further, wireless devices are going to be a big concern moving forward, a simple printer on your network is a vulnerable box. I can actually export your printer faster than I can your desktop. We have to be more secure not just looking at our PC and servers, we have to look at more devices going forward from our printers, our copiers to wireless. That is where exploits will be controlling the future. People will be looking for the weakest link and those would be the weakest links within the community. Today you have to be able to remediate and have a total remediation process for people that have disconnected and quarantine those boxes before you allow them back on the network and make sure they are secure and remediated.

Mr. PUTNAM. Mr. Maiffret.

Mr. MAIFFRET. I would concur that there are many solutions being developed to help with the problem of rogue machines and remote users and things of that nature. As far as wireless goes, it is still pretty challenging because there are so many different types of wireless. There are not necessarily a lot of standards. There is everything from wireless that is used for home use and small offices to some of the more high end wireless systems to now things like cell phones running more popular operating systems which is going to create a whole new avenue of attack but for the most part on the wireless front, there are still so many going in so many dif-

ferent directions that it is hard to have standardized security on how the thing should work.

Mr. PUTNAM. Any other comments on the trend toward wireless and reconnecting to the network? We will begin with Ms. Beinhorn as we wrap up this hearing and give you the opportunity to make any comments you wish you had been asked about or any thoughts or observations from this hearing. We will go down the line and begin with you.

Ms. BEINHORN. Thank you. We are obviously very pleased to be a part of this today and we look forward to contributing in the future. We completely support your agenda for the involvement of industry and specifically the C level involvement because the buck stops there, so it should also start there and the commitment should start there.

I just want to reinforce that. I think our participation in this and other forums will be helpful to the community.

Thank you.

Mr. PUTNAM. Thank you.

Mr. Culp.

Mr. CULP. I would echo what Ms. Beinhorn said. I think we are seeing positive results from the public/private partnerships and I think we are seeing the market causing many of the needed improvements. Customers are wielding their buying power as we speak, security is not just very high on their list, it is at the very top of their list. Microsoft and the rest of our colleagues in the industry know we have to supply that and provide it and it is that market pressure that is behind many of the improvements and innovations that I and the other folks on the panel have described today.

Mr. PUTNAM. Mr. Rosenthal.

Mr. ROSENTHAL. I would thank you again for your leadership in bringing these issues to the forefront today. Beyond the six recommendations that I mentioned before as well as in my written statement, I would ask the committee and you to closely look at the impact that software products and other technology products has on critical infrastructure sectors of our Nation.

Thank you.

Mr. PUTNAM. Thank you.

Mr. Maiffret.

Mr. MAIFFRET. I think there definitely needs to be a lot of thought and research put more on the side of why we are failing. It is amazing to me if we are spending especially in the Government, $80 million a year on technology and whatever the percentage is there on security, I think there definitely needs to be a lot of analysis done. Any time we do have a failure, what went wrong, was there not a budget, was there not enough personnel, was there the right personnel and the right tools in place but there wasn't a good process to actually track what was going on and things weren't followed through to completion, basically more specifics on why the failures are actually happening if we are spending that much.

Mr. PUTNAM. Mr. Solomon.

Mr. SOLOMON. I want to thank you for inviting me today and once again commend the committee on what they are doing.

Last year I met with Mark Forman when he was head of OMB and he told me last year the Government spent approximately $1.5 billion in some form of vulnerability management with their IT budget and the agencies still got the majority of "F" at that time. Looking at what the spend is in a cycle that is getting vicious, it is going to be more expensive and you can't keep up with it. As the hackers are moving faster, we seem to be moving slower sometimes because the reaction and our time and the process from manual to automation I think has to move a lot faster with understanding from legislation what they need to do.

Common criteria we thought was a very key point and it is important to have comment period and as an industry, I think it is very important for us all to go through it but the key is agencies don't follow it sometimes. You can go through the standards but why go through the standards and all of a sudden purchase another technology that once again potentially is not going through the certification the industry should be going through.

Third and most important, the definition, we heard a lot about patch management. I think the definition from vulnerability management to patch management is getting lost. The interpretation is it is vulnerability management, patching is a subset of what you need to do as part of vulnerability management. I see from the GAO report committees talking about configuration management but a true vulnerability management cycle includes configuration and patch management as a subset of what you need to do to ensure your networks.

Thank you.

Mr. PUTNAM. Thank you all. I want to thank both of our panels of witnesses for your participation today. The knowledge and experience and observations that were shared were outstanding.

I want to thank Mr. Clay for his continued leadership and participation in these issues.

As I stated earlier, security is a process, not a destination. Hackers, cyber criminals, disgruntled insiders, corporate spies and enemy states are not going away and no hardware or software will ever be totally secure. As such, the Federal Government and the private sector must be diligent in implementing proven risk management strategies to prevent, detect and respond to information security breaches.

In the event there may be additional questions or statements for the record that we did not have time for today, the record will remain open for 2 weeks for submitted questions and answers.

Again, thank you for your support and your leadership. With that, the subcommittee stands adjourned.

[Whereupon, at 4:22 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

○