CYBER INSECURITY: HACKERS ARE PENETRATING FEDERAL SYSTEMS AND CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

APRIL 19, 2007

Serial No. 110–26

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
43–562 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
AL GREEN, Texas
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Director & Counsel*
DR. CHRIS BECK, *Senior Advisor for Science & Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
DR. DIANE BERRY, *Minority Senior Professional Staff Member*

CONTENTS

Page

APPENDIXES

CYBER INSECURITY: HACKERS ARE PENETRATING FEDERAL SYSTEMS AND CRITICAL INFRASTRUCTURE

Thursday, April 19, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY,
AND SCIENCE AND TECHNOLOGY,
Washington, DC.

the subcommittee met, pursuant to call, at 1:11 p.m., in Room 1539, Longworth House Office Building, Hon. James Langevin [chairman of the subcommittee] presiding.

Present: Representatives Langevin, Lofgren, Etheridge, Green, Mccall, and Lungren.

Mr. LANGEVIN. [Presiding.] The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure."

Good afternoon, and welcome to the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology hearing on the hacking of federal systems and privately owned critical infrastructure.

I would like to begin by thanking the witnesses who appear before us today, and I appreciate your testimony today that we are about to hear.

I will focus my remarks this afternoon on our first panel, which will discuss the security of information technology on the federal level.

Let me be clear about the threat to our federal systems: I believe the infiltration by foreign nationals of federal government networks is one of the most critical issues confronting our nation. The acquisition of our government's information by outsiders undermines our strength as a nation. If sensitive information is stolen and absorbed by our enemies, we are strategically harmed.

Over time, the theft of critical information from government servers could cost the United States our advantage over our adversaries. This is a most critical issue that we cannot afford to ignore any longer. Today we are hearing from several agencies that have experienced significant cyber attacks against their systems. These are not the only agencies experiencing problems. They are simply the only attacks that have been made public to this point.

In October 2006, hackers operating through Chinese Internet servers launched an attack on the computer system of the Bureau

of Industry and Security, BIS, at the Department of Commerce. The hackers penetrated the computers with a "rootkit" program, a form of software that allows attackers to mask their presence and then gain privileged access to the system.

In reviewing the Commerce testimony for today's hearing, I am troubled by several things. Though Commerce first learned on July 13 that its computers were infected, this was not the date of initial infection. In fact, Commerce has no idea how long the attackers were actually inside their systems, nor do they know if the attackers are still within their systems.

As far as I can tell from the responses, rogue tunnel audits, authentication changes, and complete machine rebuilds have not occurred. We are also not sure how much information was lost. Though Commerce tells us that data was not lost, data can easily be copied and sent outside through the Internet. So there is a difference here, and I want to make that distinction, between lost and information that is copied by those who have penetrated the system.

Unfortunately, Commerce isn't the only federal agency with a problem. Prior to the Commerce hack, in June 2006, hackers accessed networks at several State Department locations, including its Washington headquarters, and inside the Bureau of East Asian and Pacific Affairs. They did so by sending a socially engineered email to an employee. The employee opened the Microsoft Word document attachment, which contained an exploit code.

I am concerned about the temporary fix that State put in place. Security authorities that I have spoken with are highly dubious about the success of "temporary wrappers," as they are called, the kind which State had to put in place due to the absence of a Microsoft patch for several months. Most targeted attacks involve rootkits, which cannot be detected or stopped by a temporary wrapper. I don't understand, therefore, why State wouldn't take its entire system offline for a full kernel inspection.

In reading State's testimony, I believe they made the determination that accessibility to data is more important than confidentiality and integrity. If State really valued the latter, they would have taken the system offline and done a full wash. Both agencies insist that these attacks are less serious because they involve unclassified servers. I disagree.

As you are no doubt aware, FISMA requires federal agencies to track down and identify every device and system on an agency's network, and to make sure that the network topology is fully described. As we learned last week, both State and Commerce received F's in the latest round of FISMA scores.

According to page 10 of the fiscal year 2006 FISMA report to Congress, the inspector general at State reported that the agency did not complete at least 50 percent of its system inventory. The I.G. at Commerce certifies that at least 96 percent of Commerce systems have been inventoried.

I will suggest to our panelists today that if they can't certify their network topologies to FISMA, then they can't know for certain that these incidents don't involve the classified networks. Furthermore, just because attacks are occurring on the unclassified network does not mean this isn't sensitive information. Information

that may be deemed classified in the future may first appear in an unclassified network.

But this isn't just about Commerce and State. I have to say that I am disappointed and troubled with the Department of Homeland Security's progress in securing cyberspace. The department is the agency responsible for securing the nation's critical infrastructure, and yet they received a D this year on its FISMA score. It is the first time since 2003 that the department did not receive an F, so I guess we are making some progress.

Our issue today is with the NCSD, but I will be honest with you: I don't know how the department thinks it is going to lead this nation in securing cyberspace when it can't even secure its own networks. Not only are these grades embarrassing, but they are dangerous. Think about all of the critical information the department is keeping on its networks. I can assure everyone here that the kinds of questions that have been asked to the State Department and the Commerce Department will be asked of DHS as well.

With regard to NCSD's response to these incidents, I have a few thoughts. It is my understanding that NCSD does not adequately share commonalities of attack information with other agencies that may be at risk. For instance, an agency like Commerce or State that has been hacked by a "zero-day exploit" will provide this information to the NCSD. But the NCSD can't just sit on that information. We need the NCSD to be the group that fuses information from across the federal government together and distributes the product for agencies to use across government.

Unfortunately, I understand that NCSD does not have protocols in place to share this kind of information with other agencies in the federal government or perform that level of work. This subcommittee will continue to monitor these issues to ensure that information sharing and technical response improves.

In closing, I think these incidents have opened a lot of eyes in the halls of Congress. We don't know the scope of our networks. We don't know who is inside our networks. We don't know what information has been stolen. We need to get serious about this threat to our national security.

That is the end of my statement.

The chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, for an opening statement.

Mr. MCCAUL. Thank you, Mr. Chairman.

I want to thank you for holding this hearing. It is a very, very important issue. It is an issue that, in my view, is overlooked many times. It poses a very significant threat to this nation. In my judgment, it can cause far greater destruction than, say, a dirty bomb which we tend to focus on quite a bit, if you think about the networks, the cyber systems, the power grids being shut down in this nation.

We know that our own military has tremendous capability and capacity to do these things. Imagine that capability in the hands of a rogue nation or a terrorist state, and what havoc they could wreak upon this country. There is espionage hacking, stealing intellectual property, and then there is a potential terrorist attack. These are all threats I take very seriously as a great threat to this nation.

VerDate Nov 24 2008 07:50 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-26\43562.TXT HSEC PsN: DIANE

Again, I want to thank you for holding this hearing on the vulnerabilities of both government and private computer systems. They are networks that are vulnerable to malicious hacking. I agree the issue of cyber security has matured past the point of talking about it in generalities and sweeping policy statements and rhetoric. Now is the time to start focusing on specific issues such as hacking into government networks.

As everyone is aware, we depend on information technology every day. We are aware of some of the more widely known problems that face our computer networks, from spam and viruses to online attempts at identity theft. These problems cause us to waste resources and time, but to a large extent they do not pose a security threat. But hacking into computer networks, especially government computer networks, does create a very real security threat, specifically a threat to our ability to rely upon information that we have in those networks.

Our country and our government depend on information. If that information becomes untrustworthy because it is on a vulnerable computer network, governmental services and institutions could grind to a halt. Some say that as long as classified network remain protected, that national security will be preserved. Unfortunately, national security depends on more than just classified information.

For example, if Medicare records are compromised, the well-being of a large portion of our citizens would be at risk. In a similar way, if computers at the IRS were compromised, the resulting unreliability of tax records could create an administrative nightmare for many Americans. In addition, there are industrial control systems that if compromised could have a very direct and dangerous result.

Control systems are those that control facilities and processes in multiple industries across the country, such as dam spillways and electric power systems. Gaining control of these systems could create as much damage as a weapon of mass destruction.

I look forward to working with you, Mr. Chairman, to take a more comprehensive look at the threats against control systems and the viability of securing these critical infrastructure systems. While this hearing is focused on the issue of hacking into computer networks, I hope that we can also clarify the role and responsibility of the Department of Homeland Security regarding these issues.

Should the department be responsible for securing all of the government's computer networks? Or should it be merely a point of coordination for departmental computer security offices? I believe the department should be the point of leadership for cybersecurity throughout the country and lead by example, by making its networks the most secure and reliable in the country.

The department already has programs to monitor the traffic on some government networks. I look forward to a better description of them by Mr. Dixon.

Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. LANGEVIN. I thank the gentleman.

I ask unanimous consent that the gentlelady from California, Ms. Lofgren, be recognized for the purpose of an opening statement.

Ms. LOFGREN. Thank you very much, Mr. Chairman. I will be brief, as I have a conflict in about 20 minutes.

I will just first thank you for holding this hearing. I think it is very important and that we begin to pay attention once again to the cybersecurity issues that I think have been neglected for the last couple of years.

I have constituents here in the next panel, VeriSign. I wanted to welcome them to the capitol and for their statement—I have read all the statements—and to note whether this could be addressed by the witnesses. In the VeriSign statement—there is no page numbers on it—but describing Project Titan. There is a discussion of the concern about a cyber attack coupled with a physical attack, which is something that has been of great concern to me over the years.

I am interested in exploring that, either in this hearing, or if more appropriate, in a more discrete setting, but I think that is something that we need to pay some considerable attention to. I also note that the current system which provides letter grades seems to have no connection whatsoever to the actual security of the agency. That is something that I hope that we can visit.

So that we will not delay the testimony, I would just simply thank the chairman for taking me out of order and allowing me to make those comments. I yield back.

Mr. LANGEVIN. I thank the gentlelady.

Other members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

I now welcome our first panel of witnesses.

Our first witness is Mr. Gregory Wilshusen, who is the director of information security issues at GAO, where he leads information security-related issues and audits of the federal government. He has over 26 years of auditing, financial management and information systems experience. He is a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration and accounting from the University of Missouri, and an M.S. in information management from George Washington University School of Engineering and Applied Sciences.

Thank you for being here.

Our second witness is Mr. Don Reid, the senior coordinator for security infrastructure, Bureau of Diplomatic Security. Mr. Reid oversees the department's information and personnel security suitability programs, and key aspects of its network cybersecurity program. Mr. Reid's information security responsibilities include the management of classified information programs, oversight of the department's Special Security Office, the operation of the Industrial Security Program, and the investigation and resolution of security violations.

Mr. Reid served in the United States Air Force for 30 years. He earned an undergraduate degree in criminology from the University of Maryland, his master's degree in Middle East studies from the University of Utah, and completed a senior managers in government seminar at Harvard's Kennedy School of Government.

Our third witness is Mr. Dave Jarrell, the critical infrastructure protection manager at the Department of Commerce. He has focused his 27-year career as a security professional, where his focus

VerDate Nov 24 2008 07:50 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00009 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-26\43562.TXT HSEC PsN: DIANE

remains on critical infrastructure protection, contingency of operations planning, crisis and disaster recovery, I.T. education for federal agency staff, and I.T. security incident response and readiness.

His first detail while in the United States Marine Corps was the protection of the president while traveling aboard Air Force One. It was while assigned to HMX–One Marine Helicopter Squadron that David received a medal for saving the life of an infant child. In his free time, Mr. Jarrell volunteers as a firefighter emergency medical technician and fire incident and command officer, where his most senior assignment was that of fire captain.

Thank you for being here.

Our final witness is Mr. Jerry Dixon, the director of the National Cyber Security Division of the Department of Homeland Security. Mr. Dixon leads the national effort to protect America's cyber infrastructure and identify cyber threats. He works collaboratively and facilitates strategic partnerships with stakeholders in the private sector, private industry and international arena. Mr. Dixon was appointed director of the NCSD on January 7, 2007.

Before joining NCSD, Mr. Dixon was the founding director of the Internal Revenue Service's computer security instant response capability. In this role, Mr. Dixon led the operational cybersecurity capability for the IRS and developed their ability to detect and respond to protect American taxpayers' private information from security attacks. Mr. Dixon has also served as director of information security for Marriott International, a private-sector company where he led cybersecurity planning, security architecture, and security operations.

Gentlemen, again I want to thank you for being here.

Without objection, the witnesses' full statements will be inserted in the record.

I will now ask each witness to summarize their statement for 5 minutes, beginning with Mr. Wilshusen.

Welcome.

STATEMENT OF GREG WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Mr. Chairman and members of the subcommittee, thank you for inviting me to testify at today's hearing on information security over federal systems. I am joined by David Powner, director of information technology at GAO.

For many years, GAO has reported weaknesses in information security, a widespread problem with potentially devastating consequences such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information. In reports to the Congress since 1997, GAO has identified information security as a government-wide high-risk issue.

Today, I will discuss the weaknesses that persist in information security controls at federal agencies, the reporting of security incidents, and the efforts by the Department of Homeland Security to develop a cyber-threat analysis and warning capability.

Mr. Chairman, serious information security weaknesses continue to threaten the confidentiality, integrity, and availability of federal systems and information. Twenty-one of the 24 major agencies

were cited by their inspectors general or independent auditors for significant weaknesses in information systems control.

For example, 18 agencies do not have adequate access controls in place to ensure that only authorized individuals could access, view or manipulate data. Even basic controls were not consistently implemented. For example, well-known vendor supply passwords were not replaced. Users were granted access privileges that exceeded their need. Sensitive information was not always encrypted, and adequate audit logs were not always maintained.

Agencies also lacked effective physical security controls. For instance, many of the data losses that occurred at federal agencies over the past few years were a result of either physical thefts or improper safeguarding of laptops and other portable devices. An underlying cause for these reasons is that agencies have not fully implemented information security programs required by the Federal Information Security Management Act, or FISMA.

These weaknesses persist even as many agencies report increased implementation of program activities. However, until agencies effectively and fully implement these programs, federal data systems will not be sufficiently safeguarded to prevent unauthorized use, disclosure and modification.

In 2006, agencies reported a record number of security incidents to the United States Computer Emergency Readiness Team, or US–CERT, which is a unit within the Department of Homeland Security responsible for collecting such information. Although agencies have noted improvements in incident reporting procedures, inconsistencies exist across agencies.

For example, although one agency reported more than 800 incidents annually internally to law enforcement authorities, it did not report them to US–CERT. I.G.s have also reported weaknesses in agencies' incident reporting procedures.

In addition to its activities with US–CERT, the Department of Homeland Security has taken steps towards addressing our recommendations for developing a strategic analysis and warning capability for cyber attacks. It has established various initiatives to enhance analytical capabilities such as promoting intelligence sharing through the US–CERT, and deploying situational awareness tools at selected federal agencies.

We believe that with a robust, effective and strategic analysis or warning capability, the department can help agencies to reduce risks associated with security incidents. However, it has not yet fully implemented our recommendations, particularly in implementing such a capability beyond the federal government.

In summary, although agencies report increased compliance with security program activities required by FISMA, serious weaknesses persist at federal agencies and reported incidents are rising. Until agencies fully implement their information security programs, they will be exposed to increased risk of cyber attacks.

The Department of Homeland Security can help agencies mitigate these risks by developing and implementing a strategic analysis and warning capability.

Mr. Chairman, this concludes my opening statement. Mr. Powner and I will be happy to answer questions.

[The statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Proper safeguards are essential to protect systems from attackers attempting to gain access and obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems.

For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences. In reports to Congress since 1997, we have identified information security as a governmentwide high-risk issue.[1] Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[2] which permanently authorized and strengthened the information security program, evaluation, and annual reporting requirements for federal agencies.

In our testimony today, we will summarize (1)µthe continued weaknesses in information security controls at federal agencies, (2) federal agencies' reporting of information security incidents, and (3) efforts by the Department of Homeland Security (DHS) to develop a cyber threat warning and analysis capability. In preparing for this testimony, we relied on our previous reports on information security at federal agencies and the challenges faced by DHS in fulfilling its cybersecurity responsibilities. We also analyzed agencies' Inspector General (IG) reports pertaining to information security; congressional reports; the 24 major federal agencies' FISMA reports for fiscal years 2004, 2005, and 2006; the performance and accountability reports for those agencies; and the Office of Management and Budget's FISMA guidance and mandated annual reports to Congress. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Significant information security weaknesses continue to place federal agencies at risk. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies cited information security control weaknesses. An underlying cause for these weaknesses is that agencies have not fully implemented agencywide information security programs. These weaknesses persist even as many agencies report increased implementation of information security program activities. However, until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be sufficiently safeguarded to prevent unauthorized use, disclosure, and modification.

In 2006, agencies reported a record number of information security incidents to US–CERT (Computer Emergency Readiness Team)—the DHS unit responsible for collecting such information. At the same time, although agencies have noted improvements in incident reporting procedures, inconsistencies exist across agencies. For example, one agency reported no incidents to US–CERT, although it reported more than 800 incidents internally and to law enforcement authorities. IGs have also reported weaknesses in agencies' incident reporting procedures.

In addition to its activities with US–CERT, DHS has taken steps towards addressing prior recommendations for developing a strategic analysis and warning capability for cyber attacks. Specifically, DHS has established various initiatives to enhance its analytical capabilities, including intelligence sharing through US–CERT and situational awareness tools at selected federal agencies. We believe that with continued progress in addressing strategic analysis and warnings, US–CERT can further agencies' efforts to reduce risks associated with incidents. However, DHS has not yet fully implemented our original recommendations, particularly in implementing such a capability beyond the federal environment.

Background

Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence,

[1] GAO, *High-Risk Series: An Update,* GAO–07–310 (Washington, D.C.: January 2007).

[2] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2946 (Dec. 17, 2002).

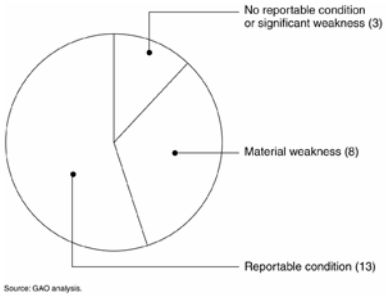
the degree of risk caused by security weaknesses is high. For example, resources (such as federal payments and collections) could be lost or stolen, data could be modified or destroyed, and computer resources could be used for unauthorized purposes or to launch attacks on other computer systems. Sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services. Finally, agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Recognizing the importance of securing federal systems and data, Congress passed FISMA, which set forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA also defined several public sector responsibilities that have been assumed by US–CERT, a partnership between DHS and the public and private sectors that was established in 2003 to coordinate defense against and responses to cyber attacks across the nation.[3] US–CERT's responsibilities include compiling and analyzing information about incidents that threaten information security and providing timely technical assistance regarding security incidents.

Significant Weaknesses Continue to Place Federal Agencies at Risk

Significant weaknesses continue to threaten the confidentiality, integrity and availability of federal information and information systems. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies indicated that deficient information security controls were either a reportable condition[4] or material weakness (see fig. 1).[5]

Figure 1: Agencies Reporting of Information Security Controls in Fiscal Year 2006 Financial Statement Audits



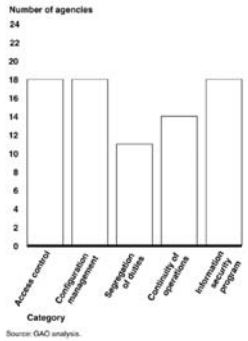
These persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 2 shows how many of the agencies had weaknesses in these five areas.

[3] FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by US–CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

[4] Reportable conditions are significant deficiencies in the design or operation of internal control that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[5] A material weakness is a reportable condition that precludes the entity's internal control from providing reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

Figure 2: Information Security Weaknesses at the 24 Major Agencies for Fiscal Year 2006



Source: GAO analysis.

Access Controls Were Not Adequate

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, can be both electronic and physical. Electronic access controls include use of passwords, access privileges, encryption, and audit logs. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft.

Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate access controls in place to ensure that only authorized individuals could access or manipulate data. Of the 24 major agencies, 18 had access control weaknesses. Such weaknesses included not replacing well-known vendor-supplied passwords, permitting excessive access privileges that users did not need to perform their jobs, not encrypting sensitive information, and not creating or maintaining adequate audit logs. Agencies also lacked effective physical security controls. For instance, many of the data losses that occurred at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Shortcomings Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include policies, procedures, and techniques addressing configuration management to ensure that software patches are installed; appropriately segregating incompatible duties; and establishing service continuity planning. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Federal agencies demonstrated weaknesses in these control areas. For example, several agencies did not always consistently install critical software patches in a timely manner, segregate duties such as security and system administration, or adequately update and test contingency plans.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for the information security weaknesses identified at federal agencies is that they have not yet fully implemented agencywide information security programs. An agencywide security program provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, promoting awareness, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

In their annual FISMA reports for fiscal year 2006, agencies reported increased compliance in several security program elements required by the law or federal policy. For example, agencies reported increases in the percentages of systems with assigned risk levels, employees receiving security awareness training, systems that

have been certified and accredited[6] and systems whose security controls were tested and evaluated.

However, our reports and those of agency IGs indicate that at least 18 of the 24 major agencies had not fully implemented agencywide programs. For example, agencies often did not effectively ensure that all employees and contractors, including those with significant information security responsibilities, received sufficient training. Also, 10 IGs rated the quality of their agencies' certification and accreditation process as "poor" or "failing" and continued to identify specific weaknesses with the process, such as incomplete risk assessments and security plans. We have also identified shortcomings in agencies' efforts in testing and evaluating the effectiveness of their information security controls. In 2006, we reported that agencies had not adequately designed and effectively implemented policies for performing such tests and evaluations.[7] Policies often did not include elements important for performing effective testing. In addition, at agencies where we examined the effectiveness of security controls, we found that they did not identify many of the vulnerabilities we identified on their systems. Further, for case studies of 30 systems at six agencies, weaknesses included insufficient testing documentation, inadequately defined assessment methods, inadequate security testing, and lack of remedial actions included in testing plans. Finally, for 16 of 24 major agencies, IGs were not able to provide assurance that their agencies almost always incorporated weaknesses for all systems into their remediation plans. Our reviews have also reported that weaknesses were not always resolved as reported, and agencies' remedial action plans did not identify resources necessary to correct weaknesses and were not always updated.

As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent unauthorized use, disclosure, and modification.

Incident Reporting Varies Across Agencies

Although strong controls may not block all intrusions and misuse, organizations can reduce the associated risks if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an organization to improve its understanding of security threats and potential costs of security incidents, as well as pinpointing vulnerabilities that need to be addressed so that they are not exploited again. When incidents occur, agencies are to notify the federal information security incident center—US–CERT.

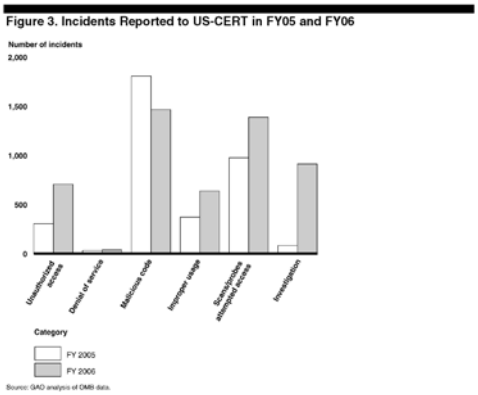
According to the US–CERT annual report for fiscal year 2006, federal agencies reported a record number of incidents, with a notable increase in incidents reported in the second half of the year. As figure 3 shows, since 2005, the number of incidents reported to US–CERT increased in every category except for malicious code. Further, a 2006 report by the House Committee on Government Reform illustrated that agencies have a wide range of incidents involving loss or theft and privacy breaches.[8] The report further indicates that the loss of personally identifiable information occurs governmentwide and is not limited to the well-publicized incident at the Department of Veterans Affairs (which involved information on about 26.5 million veterans and active duty military personnel).

---

[6] OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

[7] GAO, *Information Security: Agencies Need to Develop and Implement Policies for Periodic Testing, GAO–07–65 (Washington, D.C.: Oct. 20, 2006).*

[8] Committee on Government Reform, U.S. House of Representatives, *Staff Report: Agency Breaches Since January 1, 2003* (Washington, D.C.: Oct. 13, 2006).



Although agencies have noted many improvements in incident reporting procedures, there are still inconsistencies in reporting at various levels. For example, one agency reported no incidents to US–CERT, although it reported more than 800 incidents internally and to law enforcement authorities. Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably, information being omitted from incident reports, and reporting time requirements not being met. Without properly accounting for and analyzing security problems and incidents, agencies risk losing valuable information needed to prevent future exploits and understand the nature and cost of threats directed at them.

DHS Is Acting to Implement GAO Recommendations on Strategic Analysis and Warning, But More Actions Needed

Strategic analysis and warning is an essential element of assisting agencies in addressing information security incidents. We have previously reported that developing and enhancing a national cyber analysis and warning capability is a key DHS cybersecurity responsibility.[9] Over the last several years, we have made recommendations to DHS—as the nation's focal point for cyber critical infrastructure protection—to develop a strategic analysis and warning capability for addressing cyber attacks.[10] Accordingly, we recommended that responsible executive branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data.

DHS has taken steps towards addressing our recommendations. As we reported in 2005, DHS established various initiatives to enhance its analytical capabilities, including intelligence-sharing through US–CERT and situational awareness tools through the US–CERT Einstein program at selected federal agencies. The Einstein Program provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal civilian government. Einstein is currently deployed to nine federal agencies; US–CERT plans to deploy Einstein to an additional 10 to 15 agencies in fiscal year 2008, with a goal of deploying it to all cabinet level and critical independent federal agencies. According to DHS officials, Einstein has greatly reduced the time for the federal government to gather and share critical data on computer security risks (from 5 to 7 days to 4 to 5 hours). Further, the officials stated that Einstein has the potential to reduce data collection and information sharing to under 2 hours, allowing for vast improvements in governmental cyber response and recovery times. If properly implemented and expanded as planned, DHS's efforts in this program could strengthen its cyber threat analysis and warning capability. However, DHS has not yet fully implemented our original recommendations, particularly in implementing such a capability beyond the federal environment.

In summary, although agencies report increased compliance with security program activities required by FISMA and federal policy, serious weaknesses persist at federal agencies, and reported incidents are rising. The weaknesses exist, in part,

[9] GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO–05–434 (Washington, D.C.: May 26, 2005).

[10] GAO, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity,* GAO–06–1087T (Washington, D.C.: Sept. 13, 2006).

because agencies have not fully implemented their information security programs. Until such programs are fully implemented, agencies will be at increased risk of exposure to cyber attacks. As agencies report record numbers of incidents, inconsistencies in reporting persist. With continued progress in addressing strategic analysis and warnings, DHS's US–CERT can help agencies mitigate the risk associated with incidents.

Mr. Chairman, this concludes our statement. We would be happy to answer any questions at this time.

Mr. LANGEVIN. Thank you very much.

Mr. Reid?

STATEMENT OF DONALD REID, SENIOR COORDINATOR FOR SECURITY INFRASTRUCTURE, BUREAU OF DIPLOMATIC SECURITY, U.S. DEPARTMENT OF STATE

Mr. REID. Thank you, Mr. Chairman, Congressman McCaul and Congressman Etheridge. I am Donald Reid, the senior coordinator for security infrastructure, Bureau of Diplomatic Security at the Department of State. I am privileged to have this opportunity to testify before the subcommittee about a cyber intrusion we experienced at the department last spring.

Before discussing this intrusion in detail, I would like to inform the subcommittee generally how the State Department has structured its information technology assets to deal with cyber threats. The chief information officer employs a strategic layered approach to risk management of our information and information assets. This security strategy, which we call "defense in depth," provides the department multiple levels of defense and protection through a matrix of operational, technical and managerial security controls.

We focus on identifying and mitigating emerging threats because of our overseas exposure. Our architecture includes requisite perimeter security tools and devices, virus detection and response capability, an effective patch management program, network operations and traffic flow analysis, intrusion detection and response capability, security configuration controls, and compliance verification, to name a few.

At each of our domestic and overseas locations, we employ U.S.-citizen information systems security officers. At 10 overseas locations, we also have highly trained cybersecurity engineers. It is worth noting that the cybersecurity team at State won the National Security Agency's prestigious Frank B. Rowlett Award for its organizational excellence and information assurance in 2005, a first for the State Department.

Now, let me provide you some details about our cyber intrusion last year. In this open session, I will describe how the department responded as a team with our community of partners to a sophisticated attack, while taking care to avoid those specifics that would make it easier to harm government systems in the future.

In late May 2006, a socially engineered e-mail was sent to an employee in the East Asia Pacific region. The e-mail appeared to be legitimate and contained a Word document attachment of a congressional speech on a topic germane to this region of the world. Later analysis confirmed the attachment contained an exploit code hidden within a known Microsoft application for which there was no readily available security patch.

Once the recipient clicked on the attachment, the embedded malicious code established backdoor communications outside the department's network via a Trojan Horse. This external communication was immediately detected by our 24/7 intrusion detection system, and the department's computer incident response team was activated.

The network operations staff was directed to block communications to suspect external I.P.s and the information system security officer at post was directed to move the infected devices from the network. Additionally, we dispatched an overseas cybersecurity engineer to the post, who then began a detailed on-site analysis of the infected computers.

We also reported the malicious activity to the U.S. compute readiness team at the Department of Homeland Security. As we continued tracing the anomalous activity on our network, we identified additional intrusions and compromises, both in Washington and at other posts in the East Asia Pacific region. Our cyber analysts tested and evaluated captured malicious code and shared the results with trusted anti-virus vendors who quickly developed appropriate signatures for detecting and eradicating the malicious code.

Further analysis by our cybersecurity engineer at site and our team in D.C. led to the discovery of a second unknown vulnerability, this time in the operating system, for which no security patch existed. Homeland Security played a critical coordinating role with Microsoft, urging them to develop and deploy a brand new patch as quickly as possible.

At this stage, the CIO directed the establishment of a task force, a multi-bureau working group operating around the clock from within the secretary's operations center. The task force worked with staffs at post in their effort to mitigate the system compromises, rebuild servers, re-set passwords, and perform numerous other related tasks.

It should be noted that while the intruder's activities greatly concerned us, they did not immediately attempt to steal data. Once the network monitoring staff saw limited data being exfiltrated, Internet connectivity throughout East Asia Pacific region was immediately severed.

To develop an interim fix, we consulted with experts in industry and government, and created a temporary wrapper that would protect systems from being exploited further, but would not fix the vulnerability. The task force prescribed a remediation protocol restoring connectivity at the post that included completely sanitizing infected computers and servers, rebuilding them, changing all passwords, installing several critical patches along with the temporary wrapper, and updating anti-virus software.

The mandatory corrective actions were then confirmed via remote scans from Washington and on-site verification by post. By early July 2006, all posts were operating normally and we have not experienced similar malicious activity in our unclassified network since.

As I know you can appreciate, it is important to our overall success to handle these intrusions quietly and effectively, engaging a minimum number of players needed. We were successful here until a newspaper article telegraphed what we were dealing with. Still,

we were able to fully inform the department's oversight, intelligence and appropriations committees of the significant details of the intrusion, while at the same time the Department of Homeland Security continued to engage Microsoft to deploy the needed patch.

Mr. Chairman, I want to thank you and the subcommittee members for this opportunity, and I would be pleased to respond to your questions.

[The statement of Mr. Reid follows:]

PREPARED STATEMENT OF DONALD R. REID

Good afternoon Chairman Langevin, Congressman McCaul, and distinguished Members of the Subcommittee:

I am Donald R. Reid, the Senior Coordinator for Security Infrastructure, Bureau of Diplomatic Security at the Department of State. I am privileged to have this opportunity to testify before the Subcommittee about a cyber intrusion we experienced at the Department last spring. My statement will concentrate on events surrounding this targeted attack to the State Department's unclassified network in the May to July 2006 timeframe, how and when we detected the intrusion, who we notified and engaged to assist in defending our network, how we mitigated the damage and what improvements we have made at the Department to strengthen our cyber defenses.

Before discussing this intrusion in detail, I would like to inform the Subcommittee generally how the State Department has structured its information technology assets to deal with cyber threats. To meet the Secretary's requirement for the confidentiality, integrity, and availability of IT systems and networks in the conduct of diplomacy, the Chief Information Officer employs a strategic, layered approach to comprehensive risk management of our information and information assets. This security strategy, which we call "Defense in Depth," provides the Department multiple levels of defense and protection through a matrix of operational, technical, and managerial security controls. We focus on identifying and mitigating emerging threats because of our overseas exposure.

At the direction of former Secretary of State Powell, and embraced by Secretary Rice, the Department embarked on an aggressive program to modernize its IT systems and networks ensuring that every employee had Internet access. While Internet access can and has greatly facilitated the conduct of diplomacy, it also brings inherent risks. Our architecture includes requisite perimeter security tools and devices, virus detection and response capability, an effective patch management program, network operations and traffic flow analysis, intrusion detection and response capability, security configuration controls and compliance verification to name a few. Over our unclassified network, we daily process about 750,000 e-mails and instant messages from our more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. Also, on a daily basis, we block 500,000 spam e-mails, intercept 5,100 viruses and detect some 2,000,000 anomalous external probes to our network. At each of our domestic and overseas locations we employ U.S citizen Information System Security Officers. At 10 overseas locations, we also have highly-trained, cyber security engineers.

It is worth noting that the cyber security team at State won the National Security Agency's prestigious Frank B. Rowlett Award for its organizational excellence in information assurance in 2005—a first for the State Department. Additionally, a number of individual members have won IT community-wide recognition for their contributions and leadership. Now, let me provide you some details about our cyber intrusion last year. In this open session, I will describe how the Department responded as a team with our community of partners to a sophisticated attack, while taking care to avoid those specifics that would make it easier to harm government systems in the future.

In late May 2006, a socially-engineered e-mail was sent to an employee in the East Asia Pacific region. The e-mail appeared to be legitimate and was sent to an actual Department e-mail address. The e-mail contained a Word document attachment of a Congressional speech on a topic germane to this region of the world. Later analysis confirmed the attachment contained exploit code hidden within a known Microsoft application that took advantage of a vulnerability for which there was no readily available patch. Once the recipient clicked on the attachment the embedded malicious code established backdoor communications outside of the Department's network via a Trojan Horse. This external communication was immediately detected

by our 24/7 intrusion detection system and the Department?s Computer Incident Response Team was activated.

At this point, without full knowledge of how the exploit worked and not wanting to exacerbate the situation, network operations staff was directed to block communications to suspect external IPs and the information system security officer at post was directed to remove the infected devices from the network. In fact, we dispatched an overseas cyber security engineer to the post and began a detailed, on-site analysis of the infected computers. We also reported the malicious activity to US CERT at the Department of Homeland Security.

As we continued tracing the anomalous activity on our network, we identified additional intrusions and compromises both in Washington and other posts in the East Asia Pacific region. Our mitigation activity was continued, and we maintained effective communication with US CERT. As the State Department's cyber analysts tested and evaluated captured malicious code, they shared their results with the greater Computer Network Defense community as well as trusted anti-virus vendors. This real-time information sharing practice resulted in the anti-virus vendors quickly developing appropriate signatures for detecting and eradicating the malicious code and they deployed their results worldwide through their daily virus definition updates.

Meanwhile, critical analysis by our cyber security engineer at site and our team in D.C. led to the discovery of a previously unknown operating system vulnerability for which no security patch existed. The Department of Homeland Security played a critical coordinating role with Microsoft, urging them to develop and deploy a brand new patch as quickly as possible. State also reached out to the FBI for assistance, leveraging a well-established existing relationship.

At this stage, the CIO directed the establishment of a Task Force; a multi–Bureau working group operating around the clock from within the Secretary?s operations center. The Task Force worked with staffs at post in their efforts to mitigate the system compromises, rebuild servers, reset passwords, and performed numerous other related tasks. It should be noted while the intruders' activities greatly concerned us, they did not immediately attempt to steal data. Therefore, Task Force members proposed a set of "tripwires" for disconnecting posts from the Internet if the activity got more daring, especially if data was being stolen. Once the network monitoring staff saw limited data being exfiltrated, Internet connectivity throughout the East Asia Pacific region was immediately severed.

When it became apparent Microsoft was unable to further expedite testing and deployment of a new patch for the previously unknown vulnerability, the Department was left to develop its own interim fix. After consulting with experts in industry and government, the cyber team developed a temporary "wrapper" that would protect systems from being exploited further, but would not "fix" the vulnerability. The Task Force prescribed a remediation protocol for restoring connectivity for posts that included completely sanitizing infected computers and servers and rebuilding them, changing all passwords, installing several critical patches along with the temporary "wrapper," and updating anti-virus software. These mandatory corrective actions were then confirmed via remote scans from Washington and on-site verification by posts. By early July 2006, all posts were operating normally and we have not experienced similar malicious activity in our unclassified network since. Microsoft did deploy its patch for this exploit in August 2006.

As I know you can appreciate, it is important to our overall success to handle these intrusions quietly and effectively, engaging the minimum number of players needed. We were successful here until a newspaper article telegraphed what we were dealing with. Still, we were able to fully inform the Department's oversight, intelligence and appropriation committees of the significant details of this intrusion while, at the same time, the Department of Homeland Security continued to engage Microsoft to deploy the needed patch.

Mr. Chairman, I want to thank you and the Subcommittee members for this opportunity. I would be pleased to respond to any of your questions.

Mr. LANGEVIN. You are welcome.

Mr. Jarrell?

STATEMENT OF DAVE JARRELL, MANAGER, CRITICAL INFRASTRUCTURE PROTECTION PROGRAM, U.S. DEPARTMENT OF COMMERCE

Mr. JARRELL. Chairman Langevin, Ranking Member McCaul, and distinguished members of the subcommittee, I am David Jarrell and I represent the Department of Commerce.

I will focus my statement on how the Department of Commerce works with our technology partners to ensure the security of our systems. I will also highlight Commerce interaction with the Department of Homeland Security US–CERT. And I will brief you on the cyber incident that was discovered July 13, 2006, affecting our Bureau of Industry and Security.

Commerce security personnel work hard to protect our infrastructure and data. We exercise careful consideration in selecting and implementing technology that allows us to carry out our mission goals. With regard to protecting Commerce infrastructure, we rely on the security technology that is designed and tested by industry experts, and that adds value to the overall security posture of Commerce I.T. systems.

Information technology and industry partners provide support in the form of program and system patches. These patches are critical when new or zero-day vulnerabilities are identified. We also rely on the support of organizations like US–CERT. Commerce, like other federal government agencies, is notified by DHS US–CERT, the GFIRST, when new vulnerabilities are identified and require our attention.

Commerce manages seven computer incident response teams decentralized throughout the department, one of which supports BIS. These seven teams form the Commerce federation of computer incident response teams. To facilitate immediate notification, each team is required to report directly to US–CERT for FISMA and OMB guidance and the US–CERT concept of operations.

In regards to the BIS incident, on July 13, 2006, the BIS deputy under secretary discovered that he was unable to log onto his computer upon arrival to his office. During their investigation, BIS staff found that one BIS-infected computer attempted to access the deputy under secretary's account to no avail. It was later found that the network account was in lockout status because of the multiple unsuccessful log-in attempts. This lockout status is an automated process configured to prevent unauthorized access to BIS accounts.

Early during the investigation, Commerce notified US–CERT of the incident. BIS staff worked with the Commerce computer incident response team and our network operations staff and discovered that several other computers were involved in the incident. After being briefed on this new information, the Commerce incident response team escalated the incident, contacted US–CERT and requested on-site technical support.

As a result, two security engineers worked with Commerce to collect forensics evidence of computer drives. Commerce also provided virus-infected files to out anti-virus service provider, who in turn provided files to detect infections on BIS and other computers. Over the course of the investigation, BIS network staff continued to monitor the incident. In total, 32 BIS and one non–BIS computer were found to be infected, all of which were removed from the network and quarantined.

Throughout this process, a block list was imposed to filter and prevent access to Web sites associated with the BIS incident. These blocks and filters remain in place today. Associated website addresses and infected file names were also shared with US–CERT.

BIS management took immediate action from the time this incident was discovered. The interactive process between BIS, our network operations staff, and our incident response team enabled us to isolate infected computers.

We received timely and useful support from US–CERT, the GFIRST, and our antivirus providers. We have no evidence to believe that BIS data was taken as a result of this incident, and we believe that all appropriate actions were taken. Unfortunately, hackers and malicious code continually pose threats to our computers and networks. The results are sometimes unpredictable. That said, our I.T. security and operations staff are ready to face the challenge.

Thank you for the opportunity to appear before the subcommittee today. I am happy to answer any questions.

[The statement of Mr. Jarrell follows:]

PREPARED STATEMENT OF DAVID E. JARRELL

Chairman Langevin, Ranking Member McCaul, Chairman Thompson, Ranking Member King, and distinguished members of the Subcommittee, I appreciate the opportunity to address you on the state of cyber security protecting the Department of Commerce (Commerce).

The Commerce Information Technology (IT) security program ensures that adequate controls are in place to protect the confidentiality, integrity, and availability of non-national security and national security IT systems and the data they process, transmit, and store. To fulfill the Departments requirements under the Federal Information Security Management Act (FISMA) of 2002, the IT Security Program establishes a framework of policies and procedures consistent with government-wide laws and regulations, ensures systems are categorized and assessed for risk of harm, conducts periodic monitoring of control effectiveness, monitors tracking and completion of corrective actions, and trains personnel with IT security responsibilities.

Commerce consists of 13 bureaus that support its mission goals and objectives. This written testimony and my oral testimony will focus on the cyber intrusion affecting the Department's Bureau of Industry and Security (BIS), Commerce coordination with the Department of Homeland Security (DHS), United States—Computer Emergency Readiness Team (US–CERT), and the Department of State (State), and will offer a broad perspective of the Commerce IT security program.

PREVENTIVE MEASURES & SECURITY POSTURING

Commerce and its bureaus work diligently to ensure a sound and comprehensive IT security program. To that end, Commerce IT personnel ensure compliance with Federal requirements such as the FISMA, Office of Management and Budget (OMB) Circular A–130, Appendix III, Security of Federal Automated Information Resources, Government Accountability Office (GAO) guidance, as well as guidance issued for use within Federal civilian government Departments and Agencies and throughout the IT system development life cycle. That guidance comes in the form of National Institute of Standards and Technology (NIST) Special Publications. Other guidance considered when designing and deploying operational IT systems is derived from industry services, capabilities, and best practices.

IT systems designed to support the business needs of the Department are typically managed within the program for which they will be utilized. The systems are also reviewed by the Department's Chief Information Officer (CIO) Council and/or Commerce IT Review Board (CITRB) before funding and other resources are allocated to support the system's development and integration into the Commerce infrastructure. It is this scrutiny that senior IT staff use to determine if adequate security planning and controls are integrated into the system development life cycle (SDLC) and enterprise architecture. In addition, other security measures are integrated into the design, implementation, and operation of all IT systems within Commerce.

Commerce's enterprise architecture and IT Security Program Policy and Minimum Implementation Standards require the integration of security infrastructure for in-depth control, both at the perimeter and within the program's infrastructure. Examples of the infrastructure include the use of robust router and firewall technology, vulnerability scans and penetration testing of IT systems, monitoring of firewall and

Intrusion Detection and Prevention System logs, email filtering, spam filters, antivirus software, and intrusion detection and prevention systems.

A management control implemented throughout Commerce includes user awareness training programs, an important aspect of the Department's first line of defense. IT security awareness consists of reminders that focus the user's attention on the concept of IT security in the user's daily routine. Awareness provides a general cognizance or mindfulness of one's actions, and the consequences of those actions. Awareness activities provide the means to highlight when a significant change in the IT security program policy or procedures occurs, when an incident occurs, or when a weakness in a security control is found. IT security training develops skills and knowledge such that computer users can perform their jobs more securely, and develop relevant and necessary security skills and competencies in those who access or manage Commerce information and resources. Commerce system users are required to take computer security training on a annual basis, and all new employees/contractors to Commerce are provided training during in-processing prior to being issued a user login. In addition, IT administrators are required to take additional training courses each year that directly apply to their work related activities. We are currently assessing the option of using an Information System Security Line of Business Shared Service Center as a general security awareness training provider. This initiative is an E-Government Line of Business, managed by the Department of Homeland Security, intending to make the Government-wide IT security processes more efficient.

In addition to intra-departmental controls and counter measures, the Department ensures that key personnel remain fully aware of U.S. Government-wide initiatives and programs that affect the operation or security of its IT systems. Commerce supports U.S. Government security response and planning committees to include the National Cyber Response Coordination Group (NCRCG), the Critical Infrastructure Protection Policy Coordination Committee (CIP PCC), and the National Communications System (NCS) Committee of Principals and Representatives (COP/COR).

COMMERCE FEDERATION OF COMPUTER INCIDENT RESPONSE TEAM

For each bureau operating within Commerce, there are established Computer Incident Response Teams (CIRTs) that provide incident response for their respective bureau. Of the 13 bureaus operating within Commerce, there are six bureaus that enable their own cyber incident response programs through the use of bureau resources, including technical staff and technology. The remaining Commerce bureaus receive cyber incident response support from the centrally managed Department of Commerce Computer Incident Response Team (DOC CIRT). The DOC CIRT continually strives to reduce incident response time and increase effectiveness.

To support this decentralized computer incident response capability, Commerce also manages a Federation of Computer Incident Response Teams—where all CIRTs within the Department are represented. This intra–Departmental forum allows all Commerce CIRTs to share information on a particular incident, discuss technology and security countermeasures, and leverage Department-wide resources in the event of a large-scale attack.

Incident reports are filed directly to the DHS US–CERT in all incidents involving Department IT resources, per FISMA, other OMB guidance, and DHS US–CERT Concept of Operations (CONOPS).

On a more global level, the DHS coordinates and manages the Government Forum of Incident Response and Security Teams (GFIRST). GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government IT systems, of which the Commerce Federation of Computer Incident Response Teams maintain membership and active participation. GFIRST members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. Through participation in the GFIRST, Commerce IT security professionals receive technical information, tools, methods, assistance and guidance on cyber issues, share specific technical details regarding incidents within a trusted U.S. government environment on a peer-to-peer level, and improve incident response operations.

Initial BIS Incident Response and Reporting

Following the Department's guidance on reporting cyber incidents, BIS worked with the Network Operations Center (NOC), and the DOC CIRT to investigate suspicious behavior on BIS logical segment of the Commerce network, and its workstations. After the BIS and Commerce NOC staff confirmed that three workstations exhibited suspicious behavior, and removed them from the network, and BIS formally reported to the DOC CIRT that a breach of security occurred. As a result of this notification, the DOC CIRT notified the Director, IT Security, Infrastructure and Technology, the CIO, and the Network Operations Center (NOC),

which manages the infrastructure and "back bone" network on which BIS Internet traffic traverses. The DOC CIRT also notified the US–CERT and the Department's Office of the Inspector General (OIG).

The BIS cyber incident was discovered when the BIS Deputy Under Secretary discovered that he was unable to log into his computer upon arrival to his office on July 13, 2006, at 8:23 a.m. He immediately notified his CIO and security team, which determined that his network account was in lock-out status because three unsuccessful attempts were made to log into his account. This event was initially handled internally within BIS until such time that system staff determined it to be more significant and a reportable incident. Once determined to be an incident, as defined by Commerce policy, it was reported to the DOC CIRT.

A timeline of events was created in support of the BIS incident from a BIS, DOC CIRT, and NOC perspective:

- July 13, 2006
  - The user arrived at work and attempted to log into his computer, but discovered that the BIS system "auto-locked" his account, because failed login attempt thresholds of three attempts were reached. This prevented the user's ability to login at 8:23 a.m.
  - The user prompted the BIS internal Help Desk and computer security team to begin an investigation of the event.
  - The BIS technical staff discovered that the cause of the account lock-out was because a BIS computer attempted to access another BIS computer resource. The computer in question also attempted to execute automated processes to access two IP addresses after business hours when the authorized user of that machine was not in the office.
  - Examination of the installed anti-virus client logs revealed detected and deleted programs installed on the workstation. These auto-delete actions initiated by the anti-virus client occurred at approximately the same time that the BIS user's account was locked-out.
  - The BIS technical team contacted the Commerce NOC and requested analysis of firewall logs for the previous night's IP traffic. During this stage of the investigation, the NOC found two additional BIS computers attempting to contact one of the questionable IP addresses.
  - All three infected BIS computers were removed from the network, powered down, and quarantined.
  - The BIS CIO contacted the Commerce CIO to brief him of the situation and circumstances surrounding the event, and to advise that a CIRT report was being written based on the information gathered during the day and evening, and would be filed consistent with Department procedures.
- July 14, 2006
  - BIS formally filed the incident report with DOC CIRT that identified three of its machines operating on the BIS local area network at 11:51 a.m.
  - The DOC CIRT captured forensic images of the infected computers. The DOC CIRT determined the cause of the user account lock-out was likely due to the use of the "net" command, which is used in Windows networked environments to connect to other network resources.
  - The DOC CIRT reported the BIS incident to the US–CERT at 11:55 a.m.
- July 19, 2006
  - The Commerce OIG was notified of the BIS incident at 3:15 p.m. by the Commerce Critical Infrastructure Protection (CIP) Manager
- July 20, 2006
  - The DOC CIRT requested assistance from McAfee, the company that provides Commerce anti-virus software, to analyze and provide support to identify suspicious files and to create new definition files for detection.
- July 21, 2006
  - The DOC CIRT submitted follow-up reports to the US–CERT with investigation status updates, and requested on-site technical assistance from the US–CERT at 11:48 a.m.
  - The CIP Manager advised the Department's Federation of Computer Incident Response Team of the BIS incident, and provided the "block list" of IP addresses identified as malicious or suspicious, as well as a list of malicious file names to be monitored.
- July 22, 2006
  - DOC CIRT received a definition file from McAfee which included unique signatures to detect the malicious files identified by the DOC CIRT on July 20, 2006
- July 25, 2006
  - The US–CERT provided on-site support to the DOC CIRT.

- The US–CERT provided the DOC CIRT with updates their initial findings based on forensic image analysis.
- The DOC CIRT requested additional assistance from McAfee to analyze and provide support to identify additional suspicious files and to create new definition files for detection.

- July 25, 2006
  - The Department of Commerce IT staff, including the DOC CIRT, continued to monitor "block list" IP addresses to ensure that unwanted and unauthorized access did not occur.
- July 26, 2006
  - DOC CIRT received definition file from McAfee with unique signatures to detect the malicious files identified by the DOC CIRT on July 25, 2006.

Throughout the course of the BIS incident investigation, blocking policies of malicious and suspicious IP addresses were imposed by the DOC CIRT, BIS technical staff, and the NOC. In addition, DOC firewall administrators and BIS technical staff reviewed archive firewall logs in an attempt to identify any previous activity fitting the characteristics of the incident. All blocks remain in place today.

In summary, Commerce and BIS became aware of the break-in to BIS computers on July 13, 2006, which was determined not to be the date of the initial infection. The firewall logs were restored from the date the incident was discovered and the preceding eight months. The DOC CIRT, BIS technical staff, and the NOC reviewed and attempted to identify the initial date of the computer system compromise, to no avail. While firewall logs were reviewed for the preceding eight months prior to detecting the BIS incident, Commerce cannot clearly define the amount of time the perpetrators were inside its BIS computers before their presence was discovered. BIS has no evidence to show that data was lost as a result of this incident.

TRACKING AND CONTAINING THE OUTBREAK

An on-going challenge faced by the Department is the ability to differentiate between real and false-positive cyber security events, given the volume of system logs and information collected that must be reviewed to determine which activities are actionable.

BIS management took immediate action from the time the cyber security "event" was identified. Upon the determination that it was an *"incident,"* BIS followed Commerce incident protocol and alerted the DOC CIRT, the NOC, and the Commerce CIP Manager. BIS management, along with others within the Department, quickly established that their initial discovery of one user account locked-out due to existing policy settings included three infected computers that attempted to establish connections with two suspicious IP addresses.

As discussed in the INITIAL BIS INCIDENT RESPONSE AND REPROTING section of this report, the incident was escalated when it was discovered that more than one computer was involved. By July 24, 2006, it was discovered that ten computers *attempted* to establish connections to six suspicious IP addresses. By August 18, 2006, through continued and aggressive monitoring by BIS, the Department's IT staff, and support from the DHS US–CERT, it was discovered that a total of 32 BIS computers and one non–BIS computer *attempted* access to eleven suspicious IP addresses, as detected by monitoring logs from the Department's firewalls. It was later found that all computers showed signs of infection.

Several of these victim computers were detected by the custom Intrusion Detection Systems (IDS) signatures put into place as part of the Commerce initial response. Of these custom signatures, several indicators were supplied by the US–CERT to create custom IDS signatures. In one notable case, a victim computer triggered a custom signature, and was immediately isolated according to the improved incident response procedures. Upon further examination, it appeared that the victim was in the process of preparing files for exfiltration, but stopped as a result of controls put in place to isolate the incident. Hence the initial actions taken by Commerce, BIS, DHS, and the US–CERT were demonstrably effective in containing the damage from the incident. Of the 330 Commerce systems that require certification and accreditation in accordance with FISMA, only two systems were affected by this incident.

FISMA and certification and accreditation (C&A) compliance offer IT management useful tools to ensure that adequate controls are considered, implemented, and tested throughout the system's life cycle. BIS did have a FISMA C&A package for its system which was reviewed by the Commerce CIO's office at the time of the incident—the security incident could have occurred regardless of FISMA and C&A status because the incident method of attack uses Internet access to exploit un-patched zero-day-attack vulnerabilities, irrespective of the commercial computer security and network monitoring tools and standard prescribed Security Test & Evaluation

(ST&E) penetration testing. This is a key point related to the BIS response, specifically the decision to segregate Internet access. It is also important to note that BIS has no evidence to indicate that BIS data has been exfiltrated or compromised.

EFFECTING CHANGE ON COMMERCE AND BIS SYSTEMS

BIS implemented host-based measures that revealed other victim computers. Additional victim computers were discovered using host-based measures identifying Trojans found dormant on the BIS logical segment of the Commerce network before they became active. Processes developed by BIS to discover and stop unauthorized activity on their network proved extremely successful.

BIS established controls to detect and flag any computer infected with variants of those files causing compromise to the BIS logical segment of the Commerce network. As a result, the DOC CIRT and the NOC were able to identify those computers infected by the same outbreak traits, which included 33 computers. The Department was able to identify and quarantine the infected 33 computers through effective collaboration between Commerce and BIS IT staff involved in the incident, the "block list" of prohibited IP addresses and sites, and other controls to stop unwanted system activity (e.g., systems downloading malicious files, systems access to malicious/suspicious sites outside the control of Commerce and BIS). Only one of the 33 infected computers was outside the control of BIS.

To ensure that the infection did not spread to other Commerce bureau computer systems, file names of the infected files and associated suspicious IP addresses were shared among the Department's Federation of Computer Incident Response Teams. After review and analysis of all system logs, no other infections or infestations were evident. In addition, all infected computer drives were quarantined from use. After sample forensic images were captured for investigative purposes, all drives were boxed and have been removed, and secured under lock and key. No data was restored from backup tape as a result of the BIS incident.

As a precautionary measure, BIS executive management required the implementation of emergency change provisions to the change management process. The change involved adding supplemental rules that created additional Virtual Local Area Networks (VLANs) assigned to BIS to segregate Internet, office automation, and export control system access, and to deny all other access for BIS VLANs. When the incident occurred, a policy was invoked to impose more stringent limits on all access to or from BIS systems, (e.g., other BIS remote sites, patch management, virus definition updates).

Custom IDS signatures capable of detecting infected files causing impact on BIS computers have remained active since the discovery of the first infected computer. These IDS safeguards, coupled with augmentation of a newly implemented Intrusion Prevention System (IPS) that monitors data streams to block and/or drop traffic based on behavior for egress and ingress to the network were instrumental in containing the damage. There is a high probability that existing backdoors, if any, to the network will be detected. In addition to safeguards put in place, BIS has added supplemental assurance by segmenting use of their logical network to ensure that computers which were connected to the BIS logical segment of the Commerce network during the attack no longer have access to the Internet—effectively segmenting computers used for BIS business processes from any Internet access. Other BIS implemented other high assurance safeguards been put in place to sustain continued and reliable operation. It is impossible to say with certainty that 100% of the infestation is eradicated from the network, but with active monitoring tools in place and an attentive IT team, there is a high probability of detection.

The DOC CIRT conducts quarterly vulnerability assessments on all devices residing on the Herbert C. Hoover Building Network (HCHBNet), which includes the BIS logical segment of the DOC network. These scans involve all devices where an IP address is assigned (e.g., server class machines, desktop computers, appliances, printers, voice phones). Internet facing systems staged on the HCHBNet Demilitarized Zone (DMZ) are also part of the quarterly vulnerability assessments. In addition to quarterly vulnerability assessments, the DOC CIRT conducts vulnerability assessments for bureaus as requested to support certification and accreditation enhancements when newly approved systems and/or network devices are ready for network integration. On average, there are approximately 14,000 checks for potential vulnerabilities factored into each assessment. Results of each assessment are shared with the bureau CIO and IT Security Officer for action. The last two quarterly scans were conducted on December 18, 2006, and again on April 13, 2007.

In supporting FISMA-required certification and accreditations, the Department spends on average between $20K and $250K for Commerce IT systems depending on the size, complexity and significance. There are a total of 330 IT systems in the Department's IT inventory. Approximations are provided since legacy systems are

sometimes retired from production while new systems are introduced. Results of each system certification and accreditation security testing exercise yields extremely valuable information to the authorizing official who is ultimately responsible for the security of their system(s). Used as an education and program enhancement tool, yield valuable information pertaining to the system's overall security posture. An itemized inventory of vulnerabilities is generated during security testing that allows the system owner to methodically address as either "quick fix" items that can be readily resolved, or as mid- to long range items requiring supplemental resources. Long-term action items are inventoried in the system's Plan of Action and Milestones (POA&M).

Security testing is applied to each system as part of the System Development Life Cycle, which ensures that adequate security controls, monitoring, and logging capabilities exist, and that the overall implementation of new technology does not weaken existing security. In addition, introduction of any change is tested in a lab setting prior to being brought before the Change Control Board (CCB) for consideration, and before final integration into the production environment is allowed.

Situational Awareness Briefings

Situational awareness briefings are a tool used by the Commerce (CIO) to allow staff to receive status updates on various issues pertaining to cyber security and incident response situations occurring within Commerce. Such situational cyber security awareness briefings come in two forms: proactive and incident response briefings.

Proactive situational awareness briefings are typically scheduled for senior and technical IT professionals on a recurring basis so that they can remain apprised of cyber threats and alerts, industry recommendations, product and vendor services and capabilities, and other variables. In the realm of cyber threats and alerts, Commerce managers are informed of newly released notifications published by the DHS/US–CERT and other "watch dog" organizations that monitor and provide status on cyber-related threats and trends. As a form of proactive briefings, the CIO coordinated briefings from the DHS/US–CERT, and the Department of Defense (DoD) Joint Task Force–Global Network Operations (JTF–GNO). These briefings allowed Commerce managers to better understand the range and magnitude of cyber-related events on a global scale and the specific impacts against U.S. government managed IT systems. In all cases, Commerce IT managers have found value in the information provided by DHS/US–CERT, and DoD JTF–GNO.

Incident Response briefings are designed to inform those charged with the management and control of IT systems and resources of a particular incident and its operational impact on an affected system, its data, and the security of the system. After the BIS incident was discovered and initial response and reporting requirements were satisfied, several meetings were scheduled for the Department's senior management so that they might better understand the cyber threats faced today. To support this initiative, several briefings were scheduled that brought together Commerce senior management, the Commerce IT Security Director, the Department of Homeland Security, US–CERT management, and DoD JTF–GNO. As a supplemental effort to learn more about incidents involving U.S. Government systems, a briefing was scheduled between Commerce and BIS IT managers, and those charged with securing the State IT systems, where a "lessons learned" discussion engaged all parties.

Information Technology Security Enahncements

Monitoring and improving the state of IT security infrastructure capabilities remains a priority for the Commerce CIO. Improvements come in the form of newly released technology and upgrades to the Department's existing infrastructure. Patch management for system and appliances are updated routinely and coordinated through a formalized CCB. These changes are introduced into a test lab environment where changes and new technology can be evaluated before they are placed in a "production" environment.

To supplement the existing IPS running in IDS mode, the Department has integrated a full scale IPS to achieve active protection at the firewall. This newer technology allows the capture and analysis of both ingress and egress traffic across the network in the event of a cyber security incident. A second, more powerful log server for faster analysis and redundant storage was procured with log analysis software to speed and refine the analysis of firewall and other system logs. In addition, firewall upgrades were enabled to allow deep application inspection of traffic, and firewall log storage was increased to allow more data storage captured from the device(s).

Minimizing cyber security incident response time is a goal that the entire Federation of Computer Incident Response Team strives to improve. Changes were recently

made that enable the DOC CIRT to gain direct read access to firewall logs, without intervention by the firewall administrators or other third parties, thus improving incident response time.

Commerce will play an active role in the Cyber Storm 2007. Cyber Storm is the U.S. DHS National Cyber Security Division (NCSD) national cyber exercise. The exercise is a unique government-led, full-scale, cyber security exercise supporting Homeland Security Presidential Directive 7. Commerce also participated in the first Cyber Storm 2006 exercise coordinated by DHS/NCSD.

Commerce is also working with DHS program managers to explore the integration of Project Einstein into Commerce managed systems. The US–CERT Einstein Program is an initiative that builds cyber-related situational awareness across the Federal government. The program monitors government agencies' networks to facilitate the identification and response to cyber threats and attacks, improves network security, and increases the resiliency of critical electronically delivered government services. Einstein leverages IT so that the US–CERT can automate the sharing of critical information across the entire Federal government. Enhanced data sharing between Federal government agencies and the US–CERT provides an advanced cyber view and analysis of the Federal government's critical cyber networks.

In 2008 the Department has budgeted $120 million for IT security. This funding is estimated by the 13 bureaus operating with Commerce for a variety of IT security related tasks, including security awareness and training, system certification and accreditation, IT security operations improvements, existing security program maintenance, contingency of operations and disaster recovery planning, and other IT security related initiatives.

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

Mr. LANGEVIN. Mr. Dixon?

STATEMENT OF JERRY DIXON, DIRECTOR, NATIONAL CYBER SECURITY DIVISION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. DIXON. Chairman Langevin, Ranking Member McCaul and members of the subcommittee, I appreciate the opportunity to address you on the National Cyber Security Division's role in detection of and response to cyber intrusions of federal computer networks. The NCSD is a component of the Office of Cybersecurity and Communications within the recently established National Protection of Programs Directorate of the Department of Homeland Security.

The very topic of this hearing on the need to coordinate and respond to cybersecurity incidents across the federal government is among Secretary Chertoff's highest priorities. The National Cyber Security Division's mandate includes analysis, watch and warning, information sharing, vulnerability reduction, aiding national recovery efforts, including working collaboratively with the public and private sectors to enhance the security of America's cyber networks and information systems.

DHS works across its component entities to address cybersecurity in a cohesive manner, as well as with our federal partners across the departments and agencies. DHS and NCSD serves as the focal point for helping government, industry and the public work together to achieve the appropriate responses to cyber threats and vulnerabilities.

The NCSD's operational arm for cybersecurity is the United States Computer Emergency Readiness Team. This team provides around-the-clock monitoring of cyber infrastructure and coordinates the dissemination of information to key constituencies, including all levels of government and industry through its national cyber alert system.

Furthermore, FISMA and OMB policy requires all federal agencies to notify US–CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information. The US–CERT played a pivotal role in response efforts to the recent incidents at the Department of Commerce and the Department of State. Both incidents highlight that the threat to government systems has shifted from opportunistic hacking to targeted cyber attacks.

These cyber attacks are sophisticated and have often led to the discovery of new vulnerabilities and applications in operating systems. As a result of these vulnerabilities, U.S–CERT works closely with those vendors whose products are affected to collaborate on fixes and mitigation strategies, which are communicated to our partners within government and industry via the national cyber alert system.

To accomplish our operational mission, US–CERT focuses on enhancing situational awareness, increasing collaboration across operational security teams, assisting with prevention or rapid containment of malicious cyber attacks, and providing for interagency coordination during a cyber event. To further enhance our incident response activities, we have members from the FBI, the United States Secret Service, and other agency liaisons that help facilitate rapid response and increase our situational awareness.

Now, to focus on the recent incidents that affected the Departments of State and Commerce. Both departments notified the US–CERT in compliance with OMB guidance, FISMA, and the US–CERT concept of operations within the required timeframes. In the Department of State incident, which involved a newly identified Microsoft zero-day vulnerability, the US–CERT immediately engaged to assist with the response efforts as soon as the report was received. In collaboration with the Department of State, US–CERT coordinated with federal agencies throughout the incidence response and recovery phase.

At the same time, US–CERT coordinated daily with the Microsoft security response center for vulnerability management, patch remediation, and public disclosure coordination. Additional technical analysis revealed this vulnerability to be more dangerous and pervasive across all Microsoft operating system platforms.

Just prior to the public release of the Microsoft security bulletin, the US–CERT and Microsoft conducted a series of briefings with federal, state and local operational security teams, chief information officers, chief information security officers, and critical infrastructure sectors. Following these briefings, the US–CERT and Microsoft jointly released public notification related to the vulnerability and the availability of a security patch.

In the incident involving the Department of Commerce, the US–CERT was notified by the Department of Commerce's operational security team. During this response effort, the US–CERT provided on-site assistance to the Department of Commerce CIRT. This enabled on-site collaboration and a rapid analysis of the event so it could be quickly contained and remediated.

The NCSD continues to conduct outreach to federal agencies to raise cybersecurity awareness with operational security teams and senior officials through its government forum of incident response

teams known as GFIRST. Moreover, the NCSD continues to work with our federal and private-sector stakeholders to identify vulnerabilities and quickly identify suspicious activity by enhancing bi-directional information sharing.

The NCSD also continues to provide cybersecurity training to further increase the number of cyber incident responders to enable agencies to quickly identify and contain emerging cyber attacks. While significant progress has been made to enhance the network security of federal departments and agencies, more can and will be done.

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

[The statement of Mr. Dixon follows:]

PREPARED STATEMENT OF JERRY DIXON

Chairman Langevin, Ranking Member McCaul and Members of the Subcommittee, I appreciate the opportunity to address you on the National Cyber Security Division's (NCSD) role in detection of and response to intrusions of Federal computer networks. The NCSD is a component of the Office of Cyber Security and Communications (CS&C) within the recently established National Protection and Programs Directorate (NPPD) of the Department of Homeland Security. Assistant Secretary for Cyber Security and Communications Gregory Garcia is responsible for the overarching mission of CS&C to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's IT and communications infrastructure. This mission is part of a larger strategy to ensure the security, integrity, reliability, and availability of our information and communications networks. Indeed, the very topic of this hearing – that is, the need to coordinate better cyber security practices across the Federal government – is among Secretary Chertoff's highest priorities.

The NCSD was created in June 2003 to serve as a national focal point for cyber security and to coordinate implementation of the *National Strategy to Secure Cyberspace* ("the *Strategy*") issued by President Bush in February 2003. The Strategy outlines a national framework of priorities, which are reflected in NCSD programs, to promote cyber security and public-private partnerships. The NCSD's mandate includes analysis, watch and warning, information sharing, vulnerability reduction, aiding national recovery efforts for critical infrastructure information systems, and working collaboratively with the public and private sectors to secure America's cyber networks, systems, and assets. DHS works across its component entities to address cyber security in a cohesive manner, as well as with our Federal partners across the departments and agencies.

The NCSD's watch and warning mechanism for cyber infrastructure is the United States–Computer Emergency Readiness Team (US–CERT). This team provides around-the-clock monitoring of cyber infrastructure and coordinates the dissemination of information to key constituencies including all levels of government and industry. DHS and NCSD/US–CERT serve as the focal point for helping government, industry, and the public work together to achieve the appropriate responses to cyber threats and vulnerabilities

A key area of focus for NCSD/US–CERT is our work with the Federal departments and agencies.

Programs and Initiatives

The NCSD/US–CERT has a number of programs and initiatives to accomplish our operational mission of coordinating improvements in the security and management of the Federal Government's information systems and networks. These programs focus on enhancing situational awareness, increasing collaboration across Federal operational security teams, preventing or quickly containing cyber incidents, and providing for inter-agency coordination during a cyber event.

The NCSD manages the Einstein program, which supports Federal agencies' efforts to protect their computer networks. Einstein provides the first situational awareness picture of the Federal Government's Internet facing networks. It enables the rapid detection of cyber attacks affecting agencies and provides Federal agencies with early incident detection. Einstein is currently deployed at ten Federal agencies

with a goal to deploy it to all Cabinet level and critical independent Federal agencies.

Einstein has greatly reduced the time for the Federal Government to gather and share critical data on computer security risks from days to hours.

Another major program is the Information Systems Security Line of Business (ISS LOB). The NCSD was designated by OMB as the managing agency for the ISS LOB, which is part of the President's Management Agenda. The ISS LOB allows all Federal departments and agencies to benefit from improved levels of cyber security, reduced costs, elimination of duplicative efforts, and improved quality of service and expertise. The program addresses four information security areas that are common across the Federal Government: Security Training, Federal Information Security Management Act (FISMA) Reporting, Emerging Security Solutions for the Lifecycle, and Situational Awareness and Incident Response.

Additionally, CS&C's mission is enhanced through the continued development of the National Response Plan (NRP). The NRP provides the structure and mechanisms for Federal support to State, local, and tribal incident managers. In coordination with other Federal agencies, CS&C has been working to provide mechanisms for improving national-level response to Information Technology and Communications incidents. The Cyber Incident Annex to the NRP provides a framework for addressing a cyber event which requires a federally coordinated response, and it formalizes the National Cyber Response Coordination Group (NCRCG) as the principal Federal interagency mechanism to coordinate preparation for and response to a national-level cyber incident. The NCRCG, co-chaired by DHS, Department of Defense, and Department of Justice, coordinates recommendations and facilitates direct actions to obtain the necessary interagency support to respond to major cyber incidents.

Through the NCSD exercise program, we regularly test our plans and procedures. In February 2006 we held the first national cyber exercise, "Cyber Storm," to examine various aspects of our operational mission. This included the activation of the NCRCG and working with other Federal agencies on cyber security response to address the exercise scenarios. Lessons learned and after action items from that effort continue to be addressed by NCSD and other participants. Progress made to improve response processes and procedures since Cyber Storm, as well as other regional exercises that we sponsor, will be measured in Cyber Storm II, which is scheduled for March 2008.

We also worked collaboratively with the Air Force, the National Institute of Standards and Technology (NIST), the Defense Information Systems Agency, the National Security Agency, and Microsoft to establish common security configurations for Windows XP and VISTA. Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information. The configurations can be found on our website and we are working with NIST to help agencies adopt them.

Finally, the US–CERT Operations Incident Handling Center provides a 24 hour a day, seven day a week watch center that conducts daily analysis and situational monitoring. The Center identifies trends and provides information on incidents and other events, as they are detected and unfold, to increase situational awareness and understanding of the current operating environment. FISMA policy requires all Federal agencies to notify US–CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information (PII).

Recent Response Efforts

The NCSD/US–CERT played a pivotal role in response efforts to the recent incidents at the Department of Commerce (DOC) and the Department of State (DOS). Both incidents highlight that the threat to government systems has shifted from opportunistic hacking to targeted cyber attacks. These cyber attacks are sophisticated and have often led to the discovery of new vulnerabilities in applications or operating systems. As a result of these vulnerabilities, NCSD/US–CERT works closely with those vendors whose products are affected to collaborate on fixes and mitigation strategies, which are communicated to our partners within government and industry via the National Cyber Alert System. These incidents highlight the need for enhanced rapid situational awareness across the Federal Government. In addition, the Einstein early watch and warning system has been implemented at the DOS and groundwork is being laid to implement Einstein at the DOC in the near future.

In both incidents, the affected Departments notified the US–CERT in compliance with OMB guidance, FISMA, and the US–CERT Concept of Operations (CONOPS) within the required timeframes. While the details of these incidents should be pro-

vided by DOS and DOC, I will discuss the effective coordination processes that were utilized to respond to these incidents. We would be happy to provide the Committee with a more detailed briefing in the appropriate setting at a later date.

In the DOS incident, which involved a newly identified Microsoft "zero-day" vulnerability, the US–CERT immediately engaged to assist with response efforts as soon as the report was received. In collaboration, the DOS and US–CERT coordinated with the National Operations Center (NOC), and other Federal agencies throughout the incident response and recovery phase. At the same time, US–CERT coordinated daily with the Microsoft Security Response Center for vulnerability management, patch remediation and public disclosure coordination.

Additional technical analysis revealed this vulnerability to be more dangerous and pervasive across all Microsoft operating system platforms. Just prior to the public release of the Microsoft Security Bulletin (MS06–040), the US–CERT and Microsoft conducted a series of briefings with Federal and State operational Incident Response and Security Teams, Chief Information Officers, Chief Information Security Officers, and critical infrastructure sectors via the Sector Coordinating Committees (SCC) and designated Information Sharing and Analysis Centers (ISAC).

Following these briefings, the US–CERT and Microsoft jointly released public notifications related to the new vulnerability and the availability of a security patch. The US–CERT released a public Technical Cyber Security Alert via the National Cyber Alert System. Additionally, we disseminated a Federal Information Notice to the Federal community, and a Critical Infrastructure Information Notice to the critical infrastructure SCCs and ISACs.

Because of the significant risk posed by this vulnerability, DHS released its first ever press release focused on cyber security recommending that all users of the Microsoft Windows Operating Systems apply the security patch as quickly as possible. This public press release, along with the significant volume of media coverage and attention it garnered, led to a highly successful rollout of a security patch. Also the US–CERT continued to monitor the Federal Government's patch status and reported those results on a weekly basis until all agencies reported they had completed their patch deployments.

In the incident involving the DOC, the US–CERT was notified by the DOC's Office of the Chief Information Officer and Cyber Incident Response Team (CIRT) in accordance with OMB guidance, FISMA, and the US–CERT CONOPS. During this response effort, the US–CERT provided on-site assistance at the request of DOC CIRT. This enabled on-site collaboration and rapid analysis of the event so it could be quickly contained and remediated. In addition, they coordinated their activities with the NOC and other Federal agencies throughout the incident response and recovery phase. As a result of this incident the DOC has expanded their response capability to an around-the-clock operation which should greatly aid in their future incident detection and response efforts.

The NCSD continues to conduct outreach to Federal agencies to raise cyber security awareness with operational security teams and senior officials through its Government Forum of Incident Response and Security Teams (GFIRST). Moreover, the NCSD continues to work with our Federal and private sector stakeholders to identify vulnerabilities and quickly identify suspicious activity by enhancing bi-directional information sharing. The NCSD also continues to provide cyber security training to further increase the number of cyber incident responders to enable agencies to quickly identify and contain emerging cyber attacks.

While significant progress has been made to enhance the network security of Federal departments and agencies, more can and will be done. Based on our ongoing programs and initiatives, the NCSD and its US–CERT are poised to continue to work towards achieving greater overall cyber security with our Federal, State, local, tribal, international, and private sector partners. It is clear from our work to date and the continuing evolution of information technology in our society that additional advancements will be required to mitigate the growing cyber security risks. Accordingly, we expect continuing dialogue with this Committee as we further understand the evolving nature of the cyber security issues.

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

Mr. LANGEVIN. Thank you.

Before I go to questions, two things first of all, procedurally.

The committee rules state that witness testimony needs to be in 48 hours in advance. All the panel members got theirs in advance, with the exception of the Department of Homeland Security. I would ask that in the future that that testimony is in 48 hours, ac-

cording to committee rules. I understand that these things have to be cleared to the White House, so it is not entirely an individual's fault. But timely submission of testimony is important because we can't do business this way without having the testimony ahead of time. Okay?

The other question I have, Assistant Secretary for Cyber Security Garcia is not in attendance today. Is there a reason that he is not joining us?

Mr. DIXON. Chairman Langevin, since my direct involvement, at the time I was the deputy director for US–CERT, and since this evolves around two specific intrusions, it was thought that it would be best since I was pretty much heavily involved with both of these situations, to be present.

Mr. LANGEVIN. Thank you. We look forward to having the assistant secretary before us in the very near future.

I thank all the witnesses for their testimony.

I remind each member that he or she will have 5 minutes to question the panel.

I would now recognize myself for 5 minutes.

I would like to begin, if I could, with Mr. Reid on the question, and I just want to a little further explore the issue of the hacker penetrations that we discussed in my opening testimony, and that you addressed in your statement.

I talked about the fact that most targeted attacks involve these rootkits, which can't be detected by temporary wrappers. You describe the use of temporary wrappers initially, and then you described another process, but it wasn't clear that you took everything offline for a long period of time and did a full kernel inspection.

I would like you to address more on that, as to how you handled the penetration once you became aware of it.

Mr. REID. Sir, I would just like to reinforce in my written testimony there was a little bit more detail than the oral statement. What we were dealing with here was two zero-day exponents, for want of a better term. So we were in unknown territory and we are trying to learn as we are going along.

Mr. Dixon can probably talk to this better than I can, but my understanding is that typically it takes Microsoft a minimum of 2 months or longer to issue a security patch. So we knew it was going to take quite a long time before we were going to be able to fix this particular vulnerability, and we needed something before then. So as I indicated in my testimony, we sought the best minds out there in the private sector and in government to try and come up with a solution.

The security wrapper was what was recommended, and we came up with a protocol for deploying that. We did take the entire system down in East Asia Pacific for about a 3-week period.

Mr. LANGEVIN. Did you do a full system wash, and then re-build?

Mr. REID. Yes, sir. We rebuilt everything, and we are scanning continuously as we are checking these things are. And then we also have available to us what we call a forensic-like tool that we developed about 3 years ago. It helps us evaluate the network even closer in a very discrete manner, so that we can tell whether there is any lingering signatures.

So we felt pretty confident that we had a new process in place. We went through it very thoroughly. Before we bring a post back up on line, as I said we did remote scans from Washington to confirm what they were telling us at post. We found a lot of inconsistencies that they hadn't done the things they said they had. We wouldn't reconnect them.

There is a business case here in terms of taking an entire system off-line. It does have to be weighed and it is an incredibly tough decision to make, but the business of the State Department in part is issuing passports, issuing visas. At all our overseas posts, you have consular officers. You have visa lines out there with people waiting to apply for visas and stuff. If you take the system off-line, all of that comes to a screeching halt, with tremendous expense and disruption of normal day-to-day business.

We felt that the risks were worth it, that we had a solution that was going to work. As I indicated, since July, we haven't had any more attacks. The Microsoft patch, by the way, did not come out until August.

Mr. LANGEVIN. Do you balance the business versus security information?

Mr. REID. It is a tough decision. I am not saying that we did this. This is a decision we take to the CIO in terms of weighing that. When do you disconnect a region from the Internet? That is an incredibly disruptive thing to do, obviously, for day-to-day business. The State Department kind of got into the connectivity to the Internet late in the game. This really occurred under Secretary Powell's watch and was endorsed by Secretary Rice. So we have been modernizing our I.T. systems, but the connection to the Internet brings with it inherent risks. There is no doubt about it.

Mr. LANGEVIN. I am not satisfied that we haven't erred more on the side of protecting national security. I know the conduct of business is obviously important, but I am concerned that there hasn't been a proper balance of weight given to protecting national security.

Mr. REID. Sir, could I offer to follow up with a written explanation of what that wrapper was, what it entailed and what protections we believe were in place?

Mr. LANGEVIN. Yes, I think that would be helpful.

Mr. REID. All right, sir.

Mr. LANGEVIN. My next question is for Mr. Dixon. FISMA requires each agency to notify US–CERT about incidents affecting the information systems. How many incidents have you been notified about in 2006 and 2007?

Mr. DIXON. Yes, sir. For fiscal year 2006, we had over 23,978 incidents, I believe, somewhere in that ballpark. And then just for fiscal year 2007 to date, we are already up to 20,000-plus incidents being reported to us.

Mr. LANGEVIN. Mr. Reid, and I will ask GAO to follow up on this as well, I mentioned in my opening statement the issue of classified versus unclassified networks. Your inspector general reported that your agency only 50 percent of your system is inventoried. This means that your network topology is incomplete as well.

Given this unknown, how can you be certain that your classified networks aren't touching your unclassified networks? Can you real-

ly know that hackers have only access to unclassified networks? Do you have an idea of how much information was compromised?

Mr. REID. On the issue of unclassified and classified networks, they are separate networks. So we are very confident that there is no bleed-over, that the hackers don't have a route into the classified network by compromising the unclassified system.

We do our scanning on both systems. We do our scanning on our unclassified systems and classified systems. We have seen no activity on our classified systems, nor has the national security community as a whole.

Mr. LANGEVIN. How is that possible if you haven't completed the topology?

Mr. REID. I don't know that we necessarily agree with the I.G. My understanding of the I.G. was that they found one system that was not reported, and that they concluded from that that they couldn't trust the rest of our inventory. We feel we have a very complete inventory, certainly far more than 50 percent of the topology.

Again, it is our scanning that does that. Our scanning goes out and touches 57,000 devices that are out there on our unclassified network. We know where they are. We know that there is more work to be done on our inventory.

Mr. LANGEVIN. Mr. Wilshusen, would you comment?

Mr. WILSHUSEN. Right. This is based upon our review of the agencies and the I.G.'s FISMA report that they are required to submit. The I.G. noted that one of the State Department's systems could not be located. Due to its methodology and the scope of its work, it concluded that the State Department did not have a complete inventory.

But certainly, one of the things to consider in terms of the separation of classified and unclassified networks is that if there are any interconnections between the two, it could raise a significant security violation. Not to say that that occurred at State Department, because we have not conducted tests at the department in reviewing the security over those two types of networks.

Mr. LANGEVIN. Do you share my concern that even if the information is "unclassified," that it could very well be sensitive information that later becomes classified that could have been compromised originally?

Mr. WILSHUSEN. Of course. Sensitive information of various different types, particularly when aggregated together, could raise the level of sensitivity to that information. There is a lot of highly sensitive information that the government retains and that you do not want out in the public domain and certainly do not want a hacker or some other group to have that information.

Mr. LANGEVIN. I agree.

The chair now recognizes the ranking member, my partner in this effort, the gentleman from Texas, Mr. McCaul, to ask some questions.

Mr. MCCAUL. I thank the chairman.

I mentioned in my opening statement, really three types of hacking that could occur, and there may be more, but one would be just for mischief purposes, say, a teenager hacking in. Another one would be espionage to try to get information, steal information, in-

tellectual property. And the third would be a direct attack on the United States, a direct attack from a rogue nation or a state sponsor of terrorism. I think the last scenario would be the gravest.

I will ask about the protocol with the military. Why don't I just ask that first? If you can't answer this in a public forum, I will grant you that. Do you have any protocol with the United States military in the event there is a perceived threat, a direct attack on the United States from a rogue nation or a state-sponsored terrorist?

Mr. REID. In terms of do we have relationships built up?

Mr. MCCAUL. A protocol?

Mr. REID. Certainly. The global network operations joint task force that is run by Strategic Command is a big player in the computer network defense community. We interrelate with them all the time. We are sharing analytical information back and forth all the time. Again, Homeland Security is a key interface for us with those relationships.

Mr. MCCAUL. Getting to the specific intrusions, Mr. Reid had one. You talked about one Mr. Jarrell, and I will get to you, Mr. Dixon. Can you comment publicly on the source of these intrusions?

Mr. REID. The chairman indicated that they had their source in China, but these are hackers. These are people intruding into our systems using a sophisticated method to do it(and e-mail with hidden malicious code. Any hacker is covering their trail. So the fact that the last place they were at was in China doesn't necessarily mean that this was a state-sponsored attack.

The community as a whole, the computer network defense community as a whole, works on this attribution issue very, very hard. It is just tough to nail these things down.

Mr. MCCAUL. So it is difficult to determine the source?

Mr. REID. Most definitely, the original source.

Mr. MCCAUL. Mr. Jarrell?

Mr. JARRELL. Yes, sir. Actually, before we discovered the incident on the BIS network, we worked closely with US–CERT, but at the same time we try to depend on multiple sources of information to be able to derive our intelligence. We work with DOD's Joint Task Force for Global Network Operations, JTFGNO. So they are aware of the issues, as well as the Department of Homeland Security, US–CERT and the GFIRST.

After we experienced the incident that we did, and we reported to US–CERT, and that is our obligation to report to U.S.–CERT, we met with both US–CERT and JTFGNO to share information so that while we don't have a protocol necessarily to deal directly with the DOD environment, we wanted to pull and derive information from them. That has proven to be useful for us, so that we can gain a more broad perspective on the incidents that were occurring, and we would be able to benefit from that process and information.

We are in a situation as well, sir, that we can't definitely say the source of the attack on those BIS computers.

Mr. MCCAUL. Mr. Dixon, you quoted a very high number of over 20,000 incidents on the federal government. Is that correct?

Mr. DIXON. Those incidents include incidents from private-sector entities as well as the government. I would say the vast majority of those incidents for last year were actually from the private sec-

tor, so they could range from malicious code to phishing, with the issue involving identify theft; malicious Web sites. A majority of those things are being reported to us from corporations, as well as home users, and are called into the US–CERT.

Again, the majority of those were last year within the private sector. This year, with the advent of reporting personally identifiable information to us, that is where we have seen a large increase based on OMB management directives to report those to us within 1 hour.

Mr. MCCAUL. Were any of those incidents attempts to hack into the computer networks of the United States Congress?

Mr. DIXON. We have worked incidents with both branches of government. We have worked with the chief information security officers on the House and the Senate side. That is pretty much it. We can talk in more detail in a different setting.

Mr. MCCAUL. I understand.

My next question is to the GAO. What is your recommendation regarding the responsibility of DHS regarding cybersecurity for the federal government? Do you see them having a role as a chief information security officer for the federal government?

Mr. WILSHUSEN. I think that would present some challenges if they were to fulfill that role. One, under current law, FISMA, it requires and gives responsibility to the director of the Office of Management and Budget to oversee and coordinate the federal implementation of information security controls, as well as coordinating the development of those standards.

FISMA also assigns specific responsibilities to the heads of agencies, and makes them specifically responsible for safeguarding the information assets under their department. Having DHS in particular, and I am not sure which individual in there, but someone at the assistant secretary level being able to compel other agencies and secretaries of other agencies could be somewhat problematic from an organizational placement of that.

In addition, it would also be appropriate that DHS first assume or assure that its own security is effective and that they have taken actions to fully and effectively implement an information security program before trying to be responsible for the full federal government.

Mr. MCCAUL. Thank you.

Mr. Chairman, are we going to have one round of questions?

Mr. LANGEVIN. If we have time, I am inclined to go for two rounds. I know we are expecting a vote soon, but I am inclined to go for a second round if our witnesses can stay.

Mr. MCCAUL. My time has expired. Thanks.

Mr. LANGEVIN. I thank the gentleman.

The chair now recognizes the gentleman from North Carolina, Mr. Etheridge, for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Let me thank you and commend you for holding this hearing. I hope this is the first of many because the issue that we are talking about is so vast and it is rapidly evolving and continues to evolve. I think all of us recognize this is going to be central to what we do in the 21st century. One hearing does nothing more than

scratch the surface of what we need to be about and stay on top of.

Mr. Jarrell, let me ask you a question. Your description of the break-in in the Commerce computers is troubling. It is troubling on many levels to me. In your testimony, you note that the date and duration of illegal access is still unknown, and the extent of information compromised may never be known.

My question is, how confident are you that the information at Commerce is now secure?

Mr. JARRELL. I am very confident, sir. The reason that we don't know the date or the source of the infection on that one account is because of our audit logs and the duration that we retain those audit logs. So it is unfortunate that we are unable to pinpoint that point of action and activity on the system.

Mr. ETHERIDGE. Have you changed the protocols on that so you will be able to know in the future?

Mr. JARRELL. We are doing that now, sir. Yes, sir.

Mr. ETHERIDGE. So I assume that would be one step you have taken to improve it.

Mr. JARRELL. Absolutely.

Mr. ETHERIDGE. All right. Let me follow that up. For example, the incident at BIS was identified by a user accessing his computer with a simple password, is my understanding. Numerous guidelines from NSA, DOD and NIST recommend at least two.

Have you implemented these recommendations for privileged personnel now? Why were they not used in the past, I guess, is the question I really ought to be asking.

Mr. JARRELL. We are looking at two-factor authentication as part of our new protocol and our new process for access to systems, including any remote access or remote administration of those systems. We are working towards meeting the intent of FISMA and the OMB guidance that we are provided. We are in the process of doing that now.

Mr. ETHERIDGE. Do you have a date where you want to have that implemented?

Mr. JARRELL. We are actually working to establish contracts with vendors that can provide that kind of technology to the Department of Commerce, so that we can deploy that throughout the entire department's 13 agencies.

Mr. ETHERIDGE. With the goal for?

Mr. JARRELL. We are hoping to have that done this fiscal year so that the contract is established, and then we would have a rollout schedule into fiscal year 2008.

Mr. ETHERIDGE. Okay. Thank you, sir.

Mr. JARRELL. Yes, sir.

Mr. ETHERIDGE. Mr. Wilshusen, is it possible to determine after an attack the full extent of the damage? For example, can logs be altered to hide the nature of the attack?

Mr. WILSHUSEN. Yes, they can. It is a very difficult process to go through and try to determine the extent and the amount of damage that could occur from such an attack, particularly if the attackers have the ability and the access to delete audit logs and other system logs.

In addition, if they are adequately masquerading their tracks, it makes it more difficult, as we have already discussed here, determine the ultimate source of the attack. So it can be difficult to do that.

Mr. ETHERIDGE. I raise that question because I think as we deal with this, we need to all get a pretty good grasp of the challenge we are facing as we put more and more data at risk. That is really what we are doing.

Mr. WILSHUSEN. Right. And also the extent to which the organization is able to determine the extent of the damage also depends upon how well that organization is logging and monitoring its networks on an ongoing basis. So that also has an impact on how prepared an agency is in order to identify and detect these types of intrusions.

Mr. ETHERIDGE. Let me ask you one additional question, before I go to Mr. Dixon. It seems to me we need to do a much better job of letting our personnel know how vulnerable we are and how important it is to have security on the station they are working on.

Mr. WILSHUSEN. That is absolutely correct. Indeed, one of the best defenses is to have security in depth. That means to have multiple layers of security from various different points of vulnerability, to include assuring that users and agency personnel are fully aware of the risk and their responsibilities in mitigating those risks and practicing safe computing.

Mr. ETHERIDGE. Thank you.

Mr. Dixon, how does the Department of Homeland Security learn of instances such as those at Commerce? And how confident are you in the department's ability to analyze and prevent such incidences?

Number two, is it possible to know the extent of our vulnerability and what can we do to increase our knowledge and reduce the threat?

Mr. DIXON. In both instances, we were notified directly by their operational security teams and made aware of the incidents. They also shared with us the technical details and the information. As we do with pretty much all incidents that are reported to us, offer our assistance to help out any way we can. If it is related to a vulnerability, especially a brand new vulnerability, we will work with the affected vendor to, one, try to see when can it be fixed, and what are the options to mitigate it.

We also communicate with the government performance and response teams which has over 400 members from all the various operational security teams across the federal government and state and local governments. We have a program called Einstein that basically, we often get asked the question, who is affected or how bad is it across the U.S. government. Sometimes this question comes from the private sector. Sometimes it is from other agencies.

The way it used to work is we would have to call each and every operational security team, leverage GFIRST, make the request—can you let us know whether you have seen this type of malicious activity. They would then, and it would take a couple of days to actually go through logs of their security infrastructure to make that determination if they were seeing it or not seeing it, report that back, and then we can report back to everybody.

Mr. ETHERIDGE. Let me interrupt—and I know I am running out of time, Mr. Chairman. I am over.

What is your budget?

Mr. DIXON. It is $97 million.

Mr. ETHERIDGE. Do you do preemptive work, rather than just reactive?

Mr. DIXON. Yes, sir. US–CERT is the operational team and then we have proactive programs across the National Cyber Security Division, like software assurance.

Mr. ETHERIDGE. Thank you, Mr. Chairman. You have indulged my going over and I appreciate that. Thank you.

Mr. LANGEVIN. I thank the gentleman.

The gentleman from Texas, Mr. Green, is recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. Thank you and the ranking member for hosting this hearing. I will be terse.

Let's start with the rootkit program. Mr. Dixon, this technology, is this something that is in the hands of your typical hacker or person who desires to perpetrate mischief?

Mr. DIXON. Yes, sir. Many types of rootkits are available for download from the Internet. They are on varying levels of skills that can be used, depending on the level of how they go about social engineering it, whether they are doing targeted e-mails to specific individuals. That tends to increase the level of sophistication because they have to have some knowledge of that organization. But a lot of these things are readily available on the Internet that can be downloaded and pushed out.

Mr. GREEN. Let's go next to the zero-day exploit. If we have such an occurrence, is it true that the communication, the means by which you communicate the actual penetration is thus far confined to the department that had the zero-day exploit? Is this true?

Mr. DIXON. When you say was it combined, actually with that particular situation with the zero-day vulnerability, we were actually trying to determine were there other victims or other folks affected, and was it in fact targeted. We actually worked with probably about five other organizations to determine, are you seeing activity characteristic of this. At the same time, we were working with the vendor. They also have their network of contacts. We were trying to see if there was any other active exploitation.

Mr. GREEN. Let me intercede and ask, is there a protocol that requires you to share this information with other agencies that have not suffered the exploit?

Mr. DIXON. We have information sharing guidance within our US–CERT concept of operations, which was vetted to an interagency process. So basically, again if this was being more actively exploited when we talked to our partners within the Department of Defense and other agencies, we would have quickly went public with this. We put basically Microsoft on notice.

However, we did not find that, and found it to be targeted, and we did not want to run the risk of somebody actually developing tools to take advantage of it. In that particular instance, it was what was called "wormable," meaning an automated script or program could have taken advantage of that vulnerability that af-

fected all Microsoft operating systems, which is why we exercised extra caution and sensitivity around that particular vulnerability.

Mr. GREEN. Final question. Let's talk about the I.P. number. This is the equivalent of a fingerprint for a computer, generally speaking. It gives you the location. It doesn't necessarily take you right to the source, but at least you get in the area, the geography of the source. Is this a fair statement?

Mr. DIXON. An I.P. address does give where the traffic might be originating from. However, a lot of organizations and corporate networks, for instance, use what is called dynamic I.P. addressing, meaning that they might get a different I.P. address every time they boot up their machine or log on on a different day.

Also, a lot of attackers tend to hide where they are coming from, so there are various points, because the Internet is global. So they can make it appear to be coming from a different source than where it really is coming from. It is very easy to hide their tracks.

Mr. GREEN. All right. Thank you. That was what I wanted to get to, the ability to mask the location by the variations of I.P.s. But is it also possible to defeat the technology in some other way? As far as throwing persons who are trying to ascertain where you are off track?

Mr. DIXON. Yes, sir. There are a number of ways to hide where you are coming from. Some actually might modify the I.P. address to do what is called modifying the traffic, and put in there a bad I.P. address. So it is not that difficult. There are actually tools out there that you can download from the Internet to facilitate making that happen. There are tools out there called "onion routing," which basically makes you pretty anonymous on the Web and from where you are coming from. So there is a lot of capability there to hide your tracks.

Mr. GREEN. Perhaps this is something that is not at your level to respond to, but is there a way, and I beg that you would just consider the question, is there a way for Congress to help you with all of these various Internet providers who are continually giving out information that is antithetical to our best interests.

Mr. DIXON. We have a process, and a great working relationship with many of the Internet service providers. To give an example, when folks had come under attack from denial of service attacks, they have been effective and instrumental in actually helping what we call "black holing" the traffic, making that traffic disappear.

Where that is really important is folks that are running electronic com making that traffic disappear. Where that is really important is folks that are running electronic commerce sites, or critical Web services. We have what is called the Internet Disruption Working Group, and we work very closely with the North American Network Operators Group.

The operational relationships that we have developed with those organizations have really been essential on tackling some of the issues that we are facing.

Mr. GREEN. Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you.

We have two votes on, and then we have the second panel coming up. We brought you all the way up here, and I would like to make productive use of the time. Would the panel be willing to stay

while we have two votes? We will come back and we have one more brief round of questions, and then go to panel two. I appreciate that.

The committee stands in recess.

[Recess.]

Mr. LANGEVIN. The meeting will come to order. I thank the witnesses for staying. We will try to wrap this up as expeditiously as possible.

I would like to turn just if I could to Mr. Jarrell for my initial question, because I want to give you the opportunity to respond to something I brought up in my opening statement. That is with respect to what your department did with respect to its administrative policies after the cyber attack had occurred. If you want to take a minute to respond to that?

Mr. JARRELL. Absolutely. As we put controls in place to identify infected computers on the BIS network, we removed those computers from access. We pulled the drives and we quarantined those drives. As a result, we did not reintroduce those to our system. They were quarantined. They remain in quarantine today for any potential forensics evidence needed to support any initiatives.

So as a result, we did not reintroduce those infected drives, but also we didn't trust the data that was stored on those drives. As a result, we did not reintroduce the information on to the network on the off-chance that it may compromise issues. So we worked from clean systems.

In addition, sir, with regard to authentication changes, we suspended all of our BIS accounts because we believe they were suspect, so we expired those accounts immediately and required that all of our users reauthenticate themselves, and we continue to do that. We went from a 90-day process for user account lifespan to now 30 days. So we are significantly more aggressive in making sure that those accounts are being used by proper authorized personnel.

In addition to that, we added a second layer of control by requiring that anyone with administrative privilege on that network requires a second level of authentication to the system. It increases our security significantly, we believe.

Mr. LANGEVIN. I appreciate you addressing this for the record. Thank you. Thank you for clarifying.

Mr. Reid and Mr. Jarrell, both of your agencies received F's on FISMA. Let's just say for exploration purposes, pretend that you both received A-pluses for this year. Would that, in your opinion, have stopped the attacks from occurring? If everything possible were done with respect to security in terms of within our capability to do it today, would that have stopped the attacks?

Mr. REID. Mr. Chairman, in my opinion, no. The socially engineered e-mail would have bypassed any CAA system, and all of our systems have been certified and accredited. We certainly knew about them, whether they were part of a formal inventory or not.

I think FISMA I believe has been in existence for 5 years now. It is a great baseline law that we clearly have more work to do with at State to be able to achieve its objectives. But there are other things going on that it is not measuring, and we feel that that is an aspect of FISMA that doesn't quite tell the whole story.

For instance, our ability to detect and respond to the intrusion, nowhere is that measured in FISMA, and yet I have some terrific capability that is there to do just that. So we feel that we have a great capability for detecting these things.

Congressman McCaul, you talked about espionage, terrorism, and other kinds of things. Well, there is a criminal threat out there also that is growing dramatically in terms of threat.

We have to be able to see these things as they come into our systems, and be able to detect them, be able to respond to them, be able to mitigate them. My belief is that FISMA doesn't measure those kinds of things very well.

Mr. LANGEVIN. Mr. Jarrell?

Mr. JARRELL. We focus a significant amount of attention on FISMA compliance through certification, accreditation, and other variables. Anytime that we can have management and our executive staff's attention on the security of our infrastructure and our data, it is a good thing, because we need more eyes on the ball.

That said, a system that has been graded as an A with full FISMA compliance and understand that the certification and accreditation process that we go through on a routine basis is a snapshot in time, meaning that that snapshot in time looks at the system as it was configured at that given time. From the next day forward, any change or the introduction of new technology or even a new user on that system, changes the variable you looked at the day before.

Again, FISMA is a great tool. It is a great asset to us to be able to look at the controls that we put in place. Incident response, zero-day vulnerabilities, those kinds of things change the process and the way that we have to look at this issue. So having FISMA is a great tool. Having the ability to put more technology in place so that we can secure that system is also as great an issue. It seems that there needs to be more of a balance between FISMA and introduction of this new technology.

Mr. LANGEVIN. Mr. Wilshusen, let me ask you, what does it say about our information security laws? Somebody can get the highest score possible on our scale, but still be vulnerable to being hacked or losing critical information.

Mr. WILSHUSEN. I think it goes and speaks to how we measure the effectiveness of security at federal agencies. Clearly, the performance measures that OMB has established and its reporting instructions for federal agencies to report under FISMA, and the reporting requirement under FISMA, focus on the performance of certain control activities. Those measures do not focus on the effectiveness of those activities.

So I kind of would mirror what Mr. Jarrell has indicated, that just performing certain activities does not necessarily mean that they are being performed effectively. And certainly with what Mr. Jarrell indicated about certified and accredited systems, just because a system is certified and accredited does not make it necessarily secure, for some of the reasons that Mr. Jarrell cited.

Certainly, I agree that the law as written has been very, very positive in improving security within the federal government, because it has raised the level of attention to information security

and assigned specific responsibilities to key officials in the government and at federal agencies.

It also is based upon key and important information security practices and processes. Those are valid(the ability to assess your risk, develop policies and procedures that are risk-based, that cost-effectively reduce those risks, assuring that your staff and contractors are appropriately trained and are made aware of the risk that they need to protect against; conducting security testing and evaluation to assess the effectiveness of your controls, and then identifying vulnerabilities and taking effective and immediate remedial actions to correct those vulnerabilities.

Those are the requirements of FISMA, among others, and those are valid today, as they were 4 1/2 years ago when it was passed. The dichotomy has kind of arranged where receiving the higher grade or doing a good job under the performance measures is more an indication of what the measures we are using to assess security implementation.

Mr. LANGEVIN. We have a lot of work to do. Thank you.

I will recognize now the ranking member, the gentleman from Texas, Mr. McCaul, for the purpose of asking questions.

Mr. MCCAUL. Thank you, Mr. Chairman.

I asked the question in the last round about the role of DHS as a chief information security officer for the federal government. If I am not recounting this correctly, let me know, Mr. Wilshusen, but your response was that until DHS can really get its own act together, you wouldn't recommend that. Is that a fair assessment? If not, why don't you answer that?

Mr. WILSHUSEN. I did not use those terms exactly.

Mr. MCCAUL. I know. I am paraphrasing.

[Laughter.]

I did say "paraphrase."

Mr. WILSHUSEN. Okay. I think that is part of it. I also think just the organizational placement of DHS versus perhaps someone in maybe the office of the president. Certainly, DHS has a very important role to play in the analysis and warning capability, and because it is ideally suited for collecting and reporting all of the security incidents within the federal government, and being able to analyze that and provide that service to other federal agencies, as well as to organizations outside of the federal government.

I would also kind of like to introduce Dave Powner here, who has been doing some work in that space.

Mr. POWNER. One other factor to consider, if you look at their roles and responsibilities, and we have done work for this committee over the years looking at DHS and the National Cyber Security Division roles and responsibilities in furthering private-sector security and working with the 17 sectors.

There is a lot of work to do. We talk a lot about the US–CERT capabilities, and they are doing some good things through their Einstein project. We need to expand those capabilities. We need to do a lot more with threat identification, coming up with national threat assessments, partnering with the private sector.

So one factor to consider, too, is given all those responsibilities and the long road ahead, if you levy that requirement on an assist-

ant secretary, you are really overburdening them. I don't think it is the time right now to do that.

Mr. MCCAUL. Mr. Dixon, do you have any comment on that?

Mr. DIXON. Right now, the CIO is responsible for the protection of the data within their networks, as well as their information technology assets. I think, again with FISMA and just to touch on the certification and accreditation process, part of FISMA also includes ongoing vulnerability assessments, penetration testing, and really managing risk within your environments.

Not just doing FISMA for the sake of reporting, but actually leveraging it as a tool in your toolkit to defend your networks, to raise awareness. When you have operational issues, the certification and accreditation information lets you know how many systems in critical applications do you have across your enterprise. It helps you to quickly assess how bad is it in my environment when we do have a malicious event.

Back to your question, I think we have a significant mission to date, being a facilitator and helping organizations tackle the issues. We were just with the CIO council yesterday for all the departments. We provide them quarterly reports of incident trends within their department. We do that quarterly and annually, as well as we take a look at here is how you sit from the rest of the government, based on reporting coming into us, showing the trends and things that are coming up; here are some potential recommendations to maybe help you tackle some of these issues that you are facing.

So again, with the amount of information that we are getting not only from government, from the private sector, and being able to provide that back to key decision makers to prioritize where they focus their efforts is an effective approach.

Mr. MCCAUL. So am I correct in saying you are actually in agreement on this, that the role of coordinator and point of contact is the preferred role for the Department of Homeland Security on this?

Mr. DIXON. I think the current role that we are playing today is effective, and our capability is continuing to mature, and there is still a lot to be done. I think that the authorities of the CIOs, the effective person that knows the business applications within their environment, for some outside entity to be able to try to get a handle on their line of business, whether it is in the tax collection business or whether it issuing Social Security numbers, passports or visas—that is a pretty tall order to take on.

Mr. MCCAUL. Another question. I think Mr. Reid talked about when you had the intrusion, you consulted with Microsoft for a patch. Could you expand on this, or Mr. Dixon, I would be interested in this from your vantage point, in terms of the coordination of the department with the private sector in securing these network systems. I would go ahead and start with you, Mr. Dixon.

Mr. DIXON. I guess I am not following the exact question. Can you clarify?

Mr. MCCAUL. In terms of coordination with the private sector, I mean, the private sector has the answers, in my view. They are on the cutting edge, not the federal government. What role have you

played or what role has the department played, or do we need to play a greater role in coordinating with the private sector?

Mr. DIXON. The private sector is an essential partner in a lot of the issues that we are facing today, whether it is an operating system vendor. If we come across activity based on our experience, if we need to get security definitions or any virus signatures pushed out there based on these types of incidents, how do you get it out to the broadest audience? The way to do that is to work with those security vendors, get them the information.

Sometimes we do it in a sensitive way. Folks don't realize it. We pass to them, here is what we are seeing. They will incorporate it into their products so that it will not only clean or quarantine or prevent further victims. Again, we take operational information we get on a routine basis, get it to the information security folks to help protect a larger enterprise, because again they are the ones that are out on the frontlines. They are the ones that have the products to get across to corporations, infrastructure operators, as well as government agencies.

Mr. MCCAUL. Mr. Reid, do you have any comment?

Mr. REID. I was just going to say, we look to DHS for that kind of support and help. They have the best relationships with Microsoft. We are up to our eyeballs in things to do anyhow. About the most clout we could have put forward would have been our CIO, possibly the under secretary for management. The reality is they already have established relationships with Microsoft. This is something that has to be dealt with as quickly as possible, and they were in the best position to do it.

Mr. MCCAUL. Yes, go ahead.

Mr. DIXON. To further that, we are partnered, obviously. Under our assistant secretary, you have the national communications system, and within that they have the national coordinating center, which is made up of a lot of the major Internet service providers and telecommunication providers. We also have direct ties with a lot of the technical vendors out there, the I.T. vendors.

We are looking to further enhance and bring more of those folks into the fold because when we are dealing with some of these issues, and again with some of these zero-days, we don't have the capacity or the expertise to really know is this something new, how bad is it. We have work with those that actually develop that software. So we are trying to bring those more into the fold to help us in that major event, and also to figure out how can we quickly mitigate it.

I think the partnership with the recent standard configurations, one is XP and VISTA, that are being promulgated in partnership with OMB, NIST, NSA, and ourselves and the Air Force, is really going to go a long ways to improving the security posture of a lot of the agencies, getting to minimum baseline security standards. Again, that was through partnerships and working with vendors.

Mr. MCCAUL. Thank you. I yield back.

Mr. LANGEVIN. The gentleman from California, Mr. Lungren, is recognized for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I wish I had been able to be here, but three different things at once is difficult. I will master that if I keep working at it.

Let me ask a more general question of all of you there. That is this, and we see this in the private sector, but I would like your observation about the federal system.

Cybersecurity is an important issue that is not always so obvious to the many people that are involved in an enterprise. You can see the various physical structures that we have to stop trucks from ramming in here and so forth, and everyone can recognize that. It is easy to tell your employees, if you see something suspicious that relates to that, do something about it.

But my suspicion is that it is much more difficult to get us trained to understand this in the cyber world from the top to the bottom. One of the things I ask CEOs in the private sector is, how seriously do you consider the issue of cybersecurity? What kind of heft do you put behind those elements of your corporation that are dealing with that?

And so I guess my question to all of you is, from your perspective, what is the level of concern that we have been able to relate to the employee base at large with respect to cybersecurity, number one.

Number two, what more do we need to do to embed that in the experience of our people?

And third, and perhaps as importantly, how seriously do the top people in the departments of the federal government take this, and what kind of a priority have they placed on it?

I would love to have observations from all of you.

Mr. WILSHUSEN. I guess I will go ahead and start.

One, I think the level of attention to information security and cybersecurity issues is definitely increasing throughout the federal government. In part, that is due to the requirements specified by FISMA, but also due to the data theft that occurred last year at the Veterans Affairs. It was that incident that affected so many individuals, or potentially could have affected so many individuals that I think it really opened up the eyes of many in the federal government throughout all the federal agencies.

During hearings that were held in response to that incident, it was estimated that it could potentially cause between $30 to maybe $50 or $100 per veterans whose information was potentially lost. When you start multiplying that by 26.5 million, that ends up to be a very large amount. So I think individuals and agencies started to realize, they, this is very important and it does have costs, not only in terms of monetary costs, but the effect on veterans and citizens if the federal government loses their information.

Subsequent to that, we noticed an up-tick in the number of incidents that have been reported, particularly at VA. So that is not to say there are more incidents, but the staff and agencies are more attuned to the need to report on those particular incidents. So I think the level of attention is increasing, in part due to those factors.

Mr. REID. I certainly agree. There is a lot more attention within the State Department to this issue, not only because of our own exploits, but because of the trends across government as a whole. Secretary Rice is a strong supporter of our initiatives in cybersecurity.

On a day-to-day basis, however, that function falls to the under secretary for management. One of the things she did was to last year reach out and bring in a new CIO at State. We have had some very dramatic changes and directions that are positive for the department.

He, in turn, reached out to an A-plus organization and brought on board a new chief information security officer, who is my colleague, John Straford, who joined me here today.

Congressman you do point to the weakest link in everything we have been talking about here, and it is the human dynamic. It gets right down to the individual, and what kind of damage can they cause intentionally or unintentionally.

So we, I am sure like other agencies, we have programs in place to try and make our employees aware, to educate those that need further education in terms of what their roles and responsibilities are in the I.T. world. We have a sanction program for monitoring their behavior on the computer and taking action if they exceed their authorities and things.

So we are trying a variety of things, but at the end of the day, it is that human factor that is very, very difficult to control.

Mr. JARRELL. I hope that some part of our I.T. security program remains invisible to the user. There are a variety of different things that I mean by that. We have intrusion detection and intrusion prevention systems that sit on our network. The user does not interact with them. And those are significant tools to ensuring the security part of our network. So we continue to maintain those kinds of issues.

There is always the FISMA variable. There is always the user awareness and the role-based training requirements that we impose on our staff when they have general access to a system, versus someone who has administrative authority to our systems, and there is a significant change in that authority that is given to that account.

So some things we want to keep behind the scenes; some things we are going to bring to the forefront. We want our users to engage us when they access our system by signing rules of behavior that talk about how they should and how they should not act on our networks, what they can and what they cannot do. We believe that those are good steps towards educating our users and keeping security at the forefront of all of the things that we are trying to deal with.

Our CIOs have made I.T. security a priority because of FISMA compliance, because of report card grades, but more importantly because of the security of our data and the infrastructure that we prepare to support and carry out our mission goals. Things like PII, personally identifiable information, get our department's highest level of attention, where we report weekly on those issues, so that our executive staff is fully aware and makes sure that our bureau agency heads are fully accountable for those issues.

Mr. LANGEVIN. I thank the gentleman.

I want to thank the panel for their testimony here today. It has been very helpful and informative. We look forward to having you back again and continuing to work on this issue together.

Thank you very much. The panel is dismissed at this point, and I call up the second panel.

I want to welcome the second panel of witnesses.

Our first witness, Mr. Aaron Turner, is the cybersecurity strategist for the Department of Energy's Idaho National Laboratories. In his role, Mr. Turner applies his experience in information security to collaborate with control systems experts, energy management engineers, and homeland security law enforcement officials to develop solutions to the cyber threats that our critical infrastructure is currently facing.

Before joining INL, Mr. Turner worked in several of Microsoft's security divisions for 7 years, including as a senior security strategist within the security technology unit, as well as the security residence manager for the Microsoft sales, marketing and service group, where he led the development of Microsoft's information security curriculum for over 22,000 of Microsoft's field staff.

Our second witness, Mr. Ken Silva, is the chief security officer for VeriSign. As VeriSign's chief security officer and vice president for networking and information security, Mr. Silva oversees the mission-critical infrastructure for all network security and production I.T. services for VeriSign. In this role, he oversees the mission-critical network infrastructure for VeriSign's three core business units: security services, registry services, and telecommunications services.

Mr. Silva's responsibilities include oversight of the technical and network security, the definitive database of over 27 million Web addresses and dot-coms and dot-nets, the world's most recognizable top-level domains. Responding to over 14 billion DNS lookups daily, the platform includes the critical infrastructure for the 13 globally deployed, global top-level domain-name servers answering domain-name system requests for all dot-com and dot-net domains and the A-route server. The Internet's "dot" is the hierarchical top of the Internet's route server system and is the most heavily utilized domain-name server.

Additionally, Mr. Silva coordinates the security oversight of VeriSign's public key infrastructure, security systems that authenticate over 500,000 merchants on the Web in VeriSign's payment gateways that handle 25 percent of all the e-commerce online transactions in North America.

I want to welcome both of you here today.

Without objection, the witnesses' full statements will be inserted into the record. I would like to ask each witness now to summarize their statement for 5 minutes, beginning with Mr. Turner.

Welcome, gentlemen.

STATEMENT OF AARON TURNER, CYBERSECURITY STRATEGIST, NATIONAL AND HOMELAND SECURITY, IDAHO NATIONAL LABORATORY

Mr. TURNER. Good afternoon. Chairman Langevin, Ranking Member McCaul and distinguished members of the Homeland Security Committee, thank you for this opportunity to address you today.

To introduce myself, my name is Aaron Turner. I have been an information security practitioner since 1994. The vast majority of

my experience was gained in responding to information security incidents in 20 countries around the world. Based on that experience, I have been invited to participate in several global information security efforts. In 7 years working in Microsoft's security divisions, I had the opportunity to participate in global information security improvement programs.

When I found out about the Idaho National Laboratory's critical infrastructure protection programs, I was immediately interested in working with the INL's talented group of control systems experts. I joined the lab in September of 2006. I continue to be impressed by the INL's unique facilities that allow large-scale testing and research. These programs that INL conducts are funded through national-level programs sponsored by the Departments of Energy, Homeland Security, and Defense.

I would like to focus my remarks on historical lessons that we have learned from complex systems that rely on technology, and how an over-reliance on technology can lead to system imbalance and subsequent corrections. The quality of life that we enjoy today is built upon the successful implementation of technology. Our society is what it is because of improvements in efficiency and productivity that technology brings us.

But when we implement technology for the sake of efficiency, without regard for vulnerabilities, the consequences can be significant. The first historical example that I would like to share is based on the financial markets of the early 20th century. Facilitated by the widespread use of technology such as the telephone and ticker-tape, it was the first time that we could create a truly national financial market. But these communications technologies did not necessarily assure equal access to information. The result of the use of communications technologies without a level playing field was the system correction of 1929.

Another example of large-scale system corrections are the Internet worm incidents of Slammer and Blaster in 2003. In the years preceding, there were widespread connections of Internet systems to each other. Without sufficient security controls for those systems, it resulted in an overall Internet system that was imbalanced, where a few individuals were able to impact millions of Internet-connected systems.

There is an important system vulnerability pattern that we need to recognize based upon these two historical examples. Usually, the system vulnerabilities always begin with small-scale exploits. Where exploit capability increases, criminals begin to extort system owners or take advantage of them economically in taking the systems hostage. As the underground hacking or attacker community takes notice of the extortions, they begin to build automated vulnerability tools that are released. This results in non-experts being able to create vulnerabilities on a wide scale for widespread system compromise.

So as we take a look at those two historical examples, where are we today with regards to control systems security? First, we should note that control systems are the technological components that automate the services that we rely on such as electricity, potable water, petroleum refining, et cetera. It is important to note that most of our nation's critical infrastructure is privately owned, and

infrastructure owners are subject to market forces and resource constraints as a result.

These pressures have resulted in reduction of human operators which oversee these control systems, and an increase in the number of these systems that are connected to networks. Looking at the research that INL has conducted over the last several years in this area, we have gone out and worked with vendors of technology and private asset owners to conduct control system security assessments that have been funded by DOE and DHS. That research is important because from those assessments, we have been able to find and understand vulnerabilities in those systems. In the field assessments that INL has conducted, we have discovered high-impact vulnerabilities exploitable by low-skill-level attackers.

Comparing the control system security situation to the vulnerability pattern I mentioned previously, where are we? In May of 2006, there was an extortion scheme perpetrated against infrastructure owners. In December of 2006, there was a release of an automated control system vulnerability tool set. Now, compared to other technology sectors, where are we with regard to control system security?

We see a fragmented market with inconsistent responses by technology vendors and infrastructure owners. Control system security is lagging behind other technology sectors by years in the approach to the problem. INL's recommendation? We need to continue to prioritize and expediently address our nation's control system security issues. The use of technology in control systems has improved efficiency without the corresponding improvements in the ability to secure these newly connected systems.

For those of us working in this area, the path is clear. We must continue to maximize cooperation among infrastructure owners and technology vendors, and understand and improve control system security across the entire life-cycle of this necessary and critical technology. While we cannot reduce the risks, we must work collaboratively to reduce the impact of the occurrences.

Thank you very much.

[The statement of Mr. Turner follows:]

PREPARED STATEMENT OF AARON R. TURNER

Chairman Langevin, Ranking Member McCaul and distinguished members of the Homeland Security Subcommittee:

I am Aaron Turner, Cybersecurity Strategist for the Department of Energy's Idaho National Laboratory (INL). In my role, I apply my experience in information security to collaborate with control systems experts, industry engineers and homeland security/law enforcement officials to develop solutions to the cyber threats that our critical infrastructure is currently facing. Before joining INL, I worked in several of Microsoft?s security divisions for seven years—including as a Senior Security Strategist within the Security Technology Unit as well as the Security Readiness Manager for Microsoft?s Sales, Marketing and Services Group where I led the development of Microsoft?s information security curriculum for over 22,000 of Microsoft's field staff. I have been an information security practitioner since 1994, designing security solutions and responding to incidents in 20 countries around the world.

INL has a dedicated critical infrastructure protection research effort focused on control system security and technology risks. The U.S. government, recognizing the need to better understand the risk posed by the challenges that come with greater reliance on technology, has supported research and testing through voluntary partnerships among asset owners and operators, system vendors and the federal government. This effort includes extensive security assessments, testing security enhance-

ments, developing risk measurement and mitigation tools, and providing security training to strengthen defenses.

We participate in multi-year programs with a team of talented people including other national labs, academia and industry, based on their best-in-class core competencies and the needs of the program. This effort is funded by the Department of Homeland Security (Control System Security Program), the Department of Energy (National SCADA Test Bed or NSTB) and the Department of Defense. INL has also worked directly with critical infrastructure asset owners to assist companies and organizations with customized security services.

The development of our nation's society and economy has been based upon our successful use of technology to improve efficiency and productivity—resulting in the quality of life that many U.S. citizens enjoy today. The implementation of technology-reliant systems has resulted in the creation of some of the most complex systems mankind has ever engineered. Key examples of these systems and their complexity include our nation's financial markets, telecommunications systems, and the national electric grid.

History provides us with consistent lessons about complex systems and the way that they can impact our society and economy when they become unstable or are subject to critical vulnerabilities. There are two historical examples that we can focus on to learn important lessons about system complexity, security vulnerabilities in those systems, and the effects of having to respond to threats to those systems in an efficient and effective manner—specifically, the events surrounding the 1929 financial markets crisis and the world-wide Internet worm events of 2003.

In order for complex systems to be efficient, they require balance. When they are out of balance is when they are most vulnerable, and instability can cause loss of confidence in the systems themselves. In financial markets, the term "correction" has been adopted to describe how an unstable situation regains its balance. Such was the case in 1929 when the introduction of technologies, such as the telephone and stock ticker, allowed for the creation of a truly national financial market. These technologies were used to assure convenient communication of information between individuals on a scale that had not been available previously. Unfortunately, the convenience of communicating information did not necessarily ensure the consistency or ethics of communication between investors. This resulted in a situation where technology facilitated the creation of a large-scale system, but a relatively small amount of people capitalized on the manipulation or control of information. The financial system rapidly went out of balance and this necessitated a large-scale correction.

Since 1929, our nation has worked to implement controls that will keep our financial markets balanced and efficient, and as a society we have assigned clear responsibility for enforcing rules to assure a balanced and sustainable financial system. Unfortunately, the maturity found in financial market controls is not present in the area of control systems security.

Just as in the events leading up to the financial crisis of 1929, there were similar indications of an upcoming service disruption in the years preceding the Internet worm incidents of 2003. The wide-scale implementation of technology resulted in the largest computer network that had ever been created. The ubiquity of Internet connectivity motivated many governments, private entities, and individuals to connect their computers to the network to take advantage of the new communication opportunities. This full-speed-ahead approach to the Internet was undertaken without any coordinated oversight or planning, and it was assumed that its use involved relatively few risks.

Previous to 2003 there was relatively little attention given to securing components connected to the Internet. Most of the efforts of security professionals were directed at securing the core network services that the Internet relied on and not the distributed components that were connected to the network, which resulted in systems that were significantly out-of-balance that impacted computer users that were connected to the Internet. The first event was the SQL Slammer Worm that compromised hundreds of thousands of computers and generated enough network traffic to interrupt Internet connectivity for most of the world?s computer users. The second event of 2003 was the Blaster Worm that infected millions of computer systems worldwide and, again, interrupted Internet service on a global scale.

The impacts of the 2003 events provide examples of how technology has already become a core part of the services that we rely on. When the Slammer worm was coursing through the Internet, Bank of America?s debit and credit card operations were impacted, denying customers the opportunity to make any transactions using their bank cards. These incidents signaled a change in the way that individuals can and do exploit system instability. While the problems with market fluctuations in

1929 resulted from thousands of people interacting with the system, the Slammer and Blaster worms were created by a small number of individuals.

The correction that resulted in the case of the 2003 incidents was a significant shift in the resources dedicated to computer and Internet security. Instead of focusing on securing just the core services, the owners of the connected components began dedicating resources to secure their own systems. Within months, technology vendors began implementing processes and technologies to enable systems to be more resilient to internet-based attacks. I look back at my participation in the design and implementation of improved technology updating services while at Microsoft and still remember the enormous challenge that we faced in the days following Slammer and Blaster. The problem of creating a system that provides universal access to updates while still allowing system owners the flexibility they need to operate predictably creates a paradox that is yet to be resolved today. Looking across the technology industry, each vendor and system owner has taken a different approach to managing the risks associated with inter-connected systems.

As a result of the current fragmented approach to assuring system resiliency, information security professionals have had to continue to shift resources as the threats and vulnerabilities constantly change from day to day, with very little time to look at the problem and limited resources to coordinate a long-term strategy. For those who are seeking a strategic view, the trend that can be identified in the cyber security realm is that the threats consistently migrate on a "path of least resistance", meaning that where one service or component may be protected, the attackers will move to another service or component, continuously searching out the easiest entry points to achieve their objectives. Examples of this shift are evident in the way that core Internet services were protected after initial denial-of-service attacks in the mid 1990s, the increased focus on operating system security after the operating systems of Internet-connected computers were attacked in the late 1990s and early 2000s, and the increase in application-specific attacks that have been seen in the last two years.

In light of the 2003 Internet worm incidents and subsequent cyber security incidents, it is important to review the current state of security of the components that make up our critical infrastructure systems.

The majority of our nation's critical infrastructure is privately owned and operated, with the asset owners being subject to market forces as they make decisions relative to the security of their systems. In the current situation where control system security issue awareness is sporadic and significant incidents have not been publicly reported, these privately-owned infrastructure systems have only rudimentary mitigations for security risks. Despite the lack of appropriate security controls, there are numerous examples where asset owners have decided to increase their dependency on technology to reduce the costs associated with having to maintain a large operating staff. This reduction in the number of qualified operators and increase in the number of connected systems has resulted in a significant increase in the vulnerabilities that we see affecting control systems today.

INL has worked through government programs, industry associations and directly with vendors and asset owners to increase security awareness. While significant progress has been made in this area, it is still in the early stages of getting vendors and asset owners across infrastructures working together. Specifically, some vendors are still producing the components that make up infrastructure systems without appropriate security controls or an over-arching security architecture. Among the early and limited successes are a group of control systems technology vendors that are cooperating through government-sponsored partnerships to improve the security of those systems. Those efforts are still mostly confined to post-development security reviews. Also, in the areas of system updates, prescriptive implementation guidance and security support processes—control system security lags significantly behind other technology sectors.

Exacerbating the immaturity of security in control systems, most of the deployed systems that compose our infrastructure today were designed and deployed prior to the wide-spread availability of networking technologies and the advent of the Internet. However, as was mentioned previously, the lack of security has not stopped asset owners from connecting those systems to the Internet to take advantage of technological efficiencies in the face of increasing competitive and resource pressures.

Today, we find ourselves at a crossroads, where millions of infrastructure components are now connected to networks, allowing hackers access to systems that were never designed to be exposed to network attacks.

While recent cyber security incidents, such as theft of personal information, denial of service attacks, and large-scale system compromise have impacted the Internet and connected computing systems, it needs to be emphasized that there has not yet

been a wide-spread focus by hackers on the control systems that underlie our nation's infrastructure. Currently, vendors, asset owners, incident responders and information security experts do not fully appreciate the potential threat that exists to our infrastructure due to the risks created by vulnerabilities in control systems technologies. The pervasive use of technology, drive to ubiquitous connectivity and reduction in human oversight in control systems has introduced critical vulnerabilities in our infrastructure. The electricity that we depend on, the water that we drink, the petroleum that we use to get from place to place and financial systems we use for trade are all at some risk of being targeted and compromised.

The NSTB program has funded 12 separate control systems security reviews, during which INL experts have found that all of the evaluated systems suffer from high-impact security vulnerabilities that could be exploitable by a low-skill-level attacker, using techniques that do not require physical access to systems. In reviewing the design and implementation of these control systems, the INL team discovered that in currently-deployed systems, enhanced security controls cannot easily be implemented while still assuring basic system functionality.

With computer attackers constantly looking for new targets, they will follow the path of least resistance, which could lead them to the control systems that underlie our infrastructure. Information security experts, such as Alan Paller of the SANS (SysAdmin, Audit, Network, Security) Institute agree that without implementing risk mitigations, control systems will continue to be vulnerable. Based on historical examples of cyber security incidents in other technology domains, the corrections will most likely begin with small-scale incidents focused on economic gain, followed by the release of publicly-available vulnerability discovery tools and then transition to large-scale incidents designed to reduce confidence in the infrastructure systems themselves.

As was reported by a government analyst in 2006 at a discussion in Williamsburg, Virginia, criminal extortion schemes have already occurred, where attackers have exploited control system vulnerabilities for economic gain. In December 2006 an automated control system vulnerability scanner was released allowing individuals with relatively little experience in control systems to quickly identify vulnerabilities. Following past correction trends, we may be on the path towards wide-spread vulnerability and exploitation.

Another cause for concern is the increasing capability of hackers. In a recent paper published by IBM, experts agreed that attackers are forming a hacking industry, an underground economy that is quickly becoming a mature industry taking advantage of economies of scale with efficient distribution and communication channels. Raimund Genes, the Chief Technical Officer of Trend Micro, has stated that this underground digital economy generated more revenue than the $26 billion that legitimate security vendors generated in 2005.

Today's "just in time" markets are more susceptible to control systems security issues, whether it is the electrical utility industry, petroleum production and refining, transportation services, or other essential services. In the limited control system reviews and testing that INL has conducted we have modeled scenarios where simplistic attacks originating from the Internet could:

- Degrade electric grid capacity
- Impact petroleum refinery processes
- Interrupt transportation networks
- Compromise potable water systems

This list is composed of a brief sampling of potential outcomes. It should also be noted that the inter-connected nature of our infrastructure increases the potential for a high-impact correction. Based on the Department of Energy's research of the post–Katrina impacts on infrastructure, the second—and third-order impacts were in sectors not directly related to the infrastructure components destroyed by the hurricane.

Comparing the capabilities of the asset owners and infrastructure technology vendors to the capabilities of the underground attacker community shows the stark contrast that exists between the attackers and the defenders. Based upon the widespread use of networked technologies observed during INL assessments, it should be noted that the complex systems that make up our nation's infrastructure are out of balance—similar to how systems were out of balance preceding the events of 2003.

The course of action that is necessary in light of the current situation must be the continued decisive, coordinated, and committed effort by government, technology vendors, and asset owners. These efforts must start with effective awareness campaigns to educate all sectors about the risks that they currently face, followed with clear guidance on minimum standards for technology components of our nation?s infrastructure. This guidance must contemplate all aspects of the technology lifecycle,

including improved development standards, implementation guidelines, operations procedures, and incident response. Good progress has been made by progressive asset owners, industry-initiated infrastructure protection leadership and by vendors willing to anticipate larger market-driven requirements for more security. The process of change will best be supported by renewed vigor in finding ways to get tools, technology and knowledge to a larger audience of asset owners and technology providers.

INL's recommendation is to continue to prioritize and expediently address the issues associated with the nation's control systems security. The use of technology in our nation's infrastructure has improved the efficiency of infrastructure operations without corresponding improvements in the ability to secure these newly connected systems. For those of us working in this area the path is clear. We must maximize cooperation among asset owners and technology vendors to understand and improve control system security across the entire lifecycle of this necessary and critical technology. While we can't reduce all risk, we must work collaboratively to reduce the impact of these occurrences.

Mr. LANGEVIN. Thank you, Mr. Turner.

Mr. Silva?

STATEMENT OF KEN SILVA, CHIEF SECURITY OFFICER, VERISIGN

Mr. SILVA. Thank you, Mr. Chairman, Ranking Member McCaul, Congressman Lungren. I thank you for the opportunity to testify today.

First, I want to commend and thank you for holding this hearing. All too often, cybersecurity is only the focus of attention after a few high-profile incidents, but it is the daily efforts by the government and private sector that ensure that we are prepared so that these attacks don't cause significant economic disruption.

Make no mistake about it, cyber attacks occur every day with increasing frequency, intensity and sophistication. For the most part, Internet users never know these incidents because the infrastructure is continually strengthened and fortified to manage them. While the Internet's infrastructure may be invisible to users, it's importance cannot be overstated.

Internet usage has grown dramatically. The dot-com bust gave the illusion that Internet growth had slowed down, but in fact it has grown at remarkable rates. At the height of the dot-com boom in 2000, for example, roughly 250 million used the Internet. Today, according to Internet World statistics, more than 1 billion users worldwide rely on the Internet.

The technology of the Internet has transformed personal communications, banking and finance, government processes and manufacturing. Twenty-five percent of America's economic value moves over network connections each day. If the Internet were to go down for just a few hours, we would lose hundreds of millions of dollars of economic activity. For those reasons, it is critical that we make protecting our Internet infrastructure a priority.

As the operator of the dot-com and dot-net domain registries, as well as the steward for two of the 13 route servers that serve as the nerve center for the Internet infrastructure, VeriSign has a unique position to observe cyber threats. The scale and scope of cyber attacks has grown dramatically over the last decade. For example, bandwidth demands to deal with cyber attacks have increased 150 times since 2000.

A look at two of the largest attacks reflects how attacks have increased. In October of 2002, the Internet community got a wake-

up call when 13 DNS route servers, which serve as the heart of the Internet addressing system, came under heavy denial-of-service attack. While the October 2002 attack slowed down the Internet, it did not cripple it.

Infrastructure providers did take steps to protect the networks to cope with this new threat, in part spurred by concern that terrorists might target the Internet. Significant bandwidth was added to manage future attacks and to decentralize the infrastructure so that a single incident could not knock out the entire route server infrastructure.

Attacks on the infrastructure did not let up, however, although the newly fortified system was far better prepared to handle them. An attack of that scale today is viewed as pretty much ordinary and commonplace. Hackers, however, have become a little bit more sophisticated. A year ago, for example, a hacker systematically disabled over 1,500 Web sites using approximately 32,000 hijacked PCs in a span of 6 weeks.

In an unfortunate twist, the very devices and increased bandwidth that make the Internet more robust and user friendly, are being co-opted to compromise the Internet. Now that computers are always on, they are easily accessible to hackers and other abusers to hijack. The increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure.

VeriSign projects that the volume of Internet attacks will increase by 50 percent in both 2007 and 2008. We now that the U.S. government takes Internet attacks very seriously. The Department of Homeland Security conducts Cyber Storm, which is the most ambitious cyber war game of its kind that tests how over 100 government agencies, organizations and private companies respond to threats on the Internet.

The private sector must also be ready. VeriSign recently announced a global initiative called Project Titan to expand and diversify its Internet infrastructure by 10 times by the year 2010. Under Project Titan, VeriSign expects to increase its capacity 10 times, from over 400 billion DNS queries a day in capacity today, to more than 4 trillion per day; substantially expand its infrastructure both domestically and internationally—we are currently in the process of globally deploying over 70 sites worldwide; and to improve the monitoring infrastructure to provide a real-time, in-depth view of the anomalous network activity, either malicious or mishap activity.

Given the increased usage and mounting threats, the Internet infrastructure must be continually fortified. Simply put, if we wait for usage to reach certain levels or attacks to take place to act, we are already too late. While the dot-com and dot-net systems currently get more than 30 billion queries a day, VeriSign believes it needs to continue to build a network infrastructure that can support 10 to 100 times that level of volume for the next few years.

What is most concerning now is a scenario where terrorist attacks on a physical structure are combined with a cyber attack. Today is the 12th anniversary of the Oklahoma City bombing. It took 168 American lives. If such an attack today were combined with a cyber incident, which could disrupt the communication net-

works of those first responders, the damage could be much more severe.

Equally concerning are the number of more subtle penetration attempts. We are literally constantly probed for vulnerabilities, and if we left our guard down for even a few moments, the slightest weakness could be exploited and damage far greater than a denial-of-service attack could occur.

I thank you for this opportunity to testify here today.

[The statement of Mr. Silva follows:]

PREPARED STATEMENT OF KEN SILVA

Good morning, Mr. Chairman and distinguished Members of the Committee. My name is Ken Silva and I serve as Chief Security Officer of VeriSign.

VeriSign operates intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. The company is headquartered in Mountain View, California and it has additional corporate facilities in Virginia, Kansas, Washington state and Massachusetts.

Thank you for the opportunity to testify today. I have a prepared statement, which I would request be inserted in the record.

First, I want to commend and thank you for holding this hearing. All too often, cyber security is only the focus of attention after high-profile incidents. But it's the daily efforts by the government and private sector that ensure that we are prepared so these attacks don't cause significant economic disruption.

And make no mistake about it, cyber attacks occur every day, with increasing frequency, intensity and sophistication. For the most part, Internet users never even know of these incidents because the infrastructure is continually strengthened and fortified to manage them.

While the Internet infrastructure may be invisible to users, its importance cannot be overstated. Internet usage has grown dramatically. The dot-com bust gave the illusion that Internet growth had slowed down, but in fact it has grown at remarkable rates. At the height of the dot-com boom in 2000, for example, roughly 250 million people used the Internet. Today, according to Internet World Stats, more than 1 billion users worldwide rely on the Internet.

The technology of the Internet has transformed personal communications, banking and finance, government process and manufacturing. Twenty-five percent of America's economic value moves over network connections each day. If the Internet were to go down for a just few hours, we would lose hundreds of millions of dollars of economic activity.

For those reasons, it is critical that we make protecting our Internet infrastructure a priority.

As the operator of the .com and .net domain registries as well as the steward for two of the 13 root servers that serve as the nerve center for the Internet infrastructure, VeriSign has a unique position to observe cyber threats.

The scale and scope of cyber attacks has grown dramatically over the last decade. For example, bandwidth demands to deal with cyber attacks have increased 150 times since 2000. A look at the two largest attacks reflects how attacks have increased.

In October 2002, the Internet community got a wake-up call when the 13 DNS root servers, which serve as the heart of the Internet addressing system, came under heavy denial of service (DoS) attack.

While the October 2002 attack slowed down the Internet, it didn't cripple it.

Infrastructure providers took steps to protect the networks to cope with this new threat, in part spurred by concern that terrorists might target the Internet. Significant bandwidth was added to manage future attacks and to decentralize the infrastructure so that a single incident could not knock out a root server. Attacks on the infrastructure did not let up, although the newly fortified system was far better prepared to handle them.

An attack of that scale today is viewed as ordinary and commonplace.

Hackers, however, have become much more sophisticated. A year ago, for example, a hacker systematically disabled over 1,500 websites using approximately 32,000 hijacked PCs. In these attacks, the hacker didn't directly attack the domain-name servers. Instead, they sent their traffic to a legitimate server with a DNS query and a forged source address. This attack was also amplified by 70x.

In an unfortunate twist, the very devices and increased bandwidth that make the Internet more robust and user friendly are being co-opted to compromise the Inter-

net. Now that computers are always-on, they are easily accessible to hackers and other abusers to hijack. The increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure. VeriSign projects that the volume of Internet attacks will increase by 50 percent in both 2007 and 2008. In addition, massive infrastructures such telephony, television, and mobile communications will migrate to the Internet.

We know that the U.S. Government takes Internet attacks very seriously. The Department of Homeland Security conducts "Cyber Storm," the most ambitious cyber wargame of its kind that tests how over one hundred government agencies, organizations and private companies respond to threats to the Internet.

The private sector must also be ready. VeriSign recently announced a global initiative called Project Titan to expand and diversify its Internet infrastructure by ten times by the year 2010.

Under Project Titan, VeriSign expects to:

- Increase its capacity 10 times from 400 billion DNS queries a day to 4 trillion a day. By doing so, VeriSign will ensure that the infrastructure is prepared not only for attacks, but the dramatic increase in Internet usage driven by Internet-enabled mobile devices and social networking applications.
- Substantially expand its infrastructure both domestically and internationally. VeriSign is in process of globally deploying over 70 DNS constellation sites. These sites will distribute Internet traffic and enable us to isolate attacks as they happen.
- Improve the monitoring infrastructure to provide a real-time, in-depth view of anomalous network activity, either malicious or mishap.

Given the increased usage and mounting threats, the Internet infrastructure must be continually fortified. Simply put, if we wait for usage to reach certain levels or attacks to take place to act, we are already too late. While the .com and .net systems currently get more than 30 billion queries a day, VeriSign believes it needs to continue to build a network infrastructure that can support 10 to 100 times that level of volume in the next few years.

What is most concerning now is a scenario where terrorist attacks on a physical structure are combined with a cyber attack. Today is the 12th anniversary of the Oklahoma City bombing that took 168 American lives. If such an attack today was combined with a cyber incident that took down or disrupted our communications networks the damage could be much more severe.

Equally concerning, are the number of more subtle penetration attempts. We are literally constantly probed for vulnerabilities and if we left our guard down for even a few moments, the slightest weakness could be exploited and damage far greater than that of a denial of service attack could occur.

We have all witnessed, and learned, a lot over the last decade. We have had tragic reminders that our critical infrastructure and national symbols are targets. We have seen how not adequately preparing for events can have disastrous consequences.

We know that Internet is often taken for granted. But the operators of that infrastructure must never take it for granted. We must remain vigilant in understanding what is driving the growth of the Internet and the malicious efforts of some who wish to disrupt it.

Thank you for the opportunity to testify here today.

Mr. LANGEVIN. Gentleman, I thank you for your testimony.

I will now recognize myself for questions, beginning with Mr. Turner.

I wanted to ask why haven't we seen a widescale event take place if these systems are so easy to access? Without widescale events, what is the motivation for users to secure them? And how do we educate the owners and operators of these systems? And finally, will the systems ever be 100 percent secure?

Mr. TURNER. Thank you for the opportunity to respond.

For your first question, why haven't we seen a major incident to date. There are a couple of factors that influence that, the first one being that for the vast life-span of these systems, they have not been connected to any network of any sort.

But as I mentioned in my testimony, the private infrastructure owners who manage these systems, they are private entities and they are subject to market forces and resource constraints. So when

they have the opportunity to reduce staff to improve efficiency, they usually defer to connecting them to some sort of network to control them remotely.

Based upon our research that we have seen and the assessments that we have conducted at INL, we see a significant increase in the number of connected systems in the last year. So we believe that we have not see a major incident to date because of the lack of connectivity, but that ecosystem is changing.

Does that address your first question?

Mr. LANGEVIN. Yes, sure.

Mr. TURNER. The second one, how to educate. There are really three parts to the awareness equation that need to be taken a look at here. This problem cannot be solved by just focusing on the infrastructure owners or just focusing on the vendors. It has to be a holistic solution. So the vendors first need to be made aware of these types of vulnerabilities very early in the life-cycle of these systems, so that these vulnerabilities are not created when the product is shipped to the customer.

Also, the customer needs to be informed about how to make sure that they deploy the systems in the correct way, and how to recognize an insecure architecture. And then the third aspect is we need to make sure that our law enforcement officials and incident responders understand what an incident looks like. We don't really have a solid understanding of what an incident in this area looks like because nothing big has happened yet.

And then the last one, how can we be 100 percent certain, or do we need to get to 100 percent security.

Mr. LANGEVIN. Will we ever get to 100 percent?

Mr. TURNER. I think, as was mentioned before in prior testimony, security is a snapshot of a moment in time. The threat always changes. The vulnerabilities are introduced. So I don't believe you can ever have a dynamic, effective, productive system and be 100 percent secure. It would violate the reason why you built it.

What you have to have in place are mitigations that help you get the business accomplished, while still monitoring the integrity of that system. So you have to make sure that you take a balanced response in making sure the system does its job, but that it can be monitored and maintained, and its integrity can be maintained over time.

Mr. LANGEVIN. Gentlemen, why do you think our nation isn't doing enough in the area of control system security? Why does the government need to get involved? Where are the leadership areas that are appropriate for government? And how can federal regulation be used to improve the CIP posture? What areas are not appropriate for government, as well as what areas are appropriate?

Mr. TURNER. Why are we not doing enough? Based upon my professional experience, I have seen what it takes to conduct a global information security program within a company like Microsoft; what it takes to make sure that the developers of the technology understand things; that the implementers understand things; and the end-customers understand it, too.

When I compare the insights that I have into the budget that a company like Microsoft spends on a global information security improvement program, and I compare that to the insight that I have

into what we are doing as a country to protect our critical infrastructure, the budget being spent by Microsoft is a magnitude order greater than what we are spending as a country in this area. So that is the first comparison that I would make.

As far as leadership, I think that government leadership should rely in areas such as setting a good example of how to secure government systems so that the critical infrastructure providers can look to the government as a leader in the space, and then also serve as a coordinator among different experts so that the expertise can be shared across the ecosystem.

The last point of your question as far as regulation, I think government should get involved to assure a level playing field. There should be minimum standards that are established so that it is clear for all of the technology vendors and the infrastructure owners what constitutes the minimum here.

I think a good example of that is some of the work that INL has done in conjunction with the DHS program for a procurement standard, meaning that you can teach the infrastructure owner what the minimum standard should be for those systems before you buy them and before you install them. We need to do that across the ecosystem, though.

Mr. LANGEVIN. Mr. Silva?

Mr. SILVA. I don't disagree with anything Mr. Turner said, except that in listening to the earlier panel and listening to some of the description of what they had to go through and how they had to do some risk analysis and make some decisions on whether to take these machines off or not, is not uncommon from what almost any company in the world would go through if they experienced a very similar type of incident.

Patch management and the ability to keep systems updated and secure, for instance you could put a computer on the network today and you have cleaned all of the vulnerabilities that you know about today. Tomorrow, there may be 200 vulnerabilities attached to that machine that you didn't know about when you put the machine on, or it could be a year from now, et cetera.

The ability to be able to keep those machines updated and patched is a challenge that this industry has been facing for a decade, and still hasn't completely solved the problem. Different companies deal with it in different ways. Trying to keep the systems secured to a common level and establishing a baseline for that, frankly that baseline would be probably obsolete by the time the ink dried on it in many cases.

A lot of our government agencies, as well as our private companies are facing a lot of compliance issues, where they are dedicating a lot of time to trying to meet somebody's interpretation of what a minimum standard is, and not adapting to what the new challenges are. So I think that there is a fine line to walk here between holding people accountable and regulating it.

Mr. LANGEVIN. Thank you.

The chair now recognizes the ranking member of the subcommittee, Mr. McCaul, the gentleman from Texas, for 5 minutes.

Mr. MCCAUL. I thank the chair.

This is kind of a big picture question, but today vulnerabilities are discovered, found. Who do you believe is responsible to lead that effort to mitigate the risk? Who takes the lead?

Mr. SILVA. Well, today, the government agency that we look to for that is the US–CERT. They are considered the authority of database for vulnerabilities and exploitation management. So we typically use them as the authoritative source for the contents of what those vulnerabilities are. They will typically list some mitigation strategies associated with that.

Mr. MCCAUL. Do you believe that they are providing that leadership today at an adequate level? Is there more that they could be doing?

Mr. SILVA. Well, I think that there is always more anybody could be doing, but yes I do think that they are actually doing a pretty good job at that. As a matter of fact, I think that when you look at the NCSD, for example, okay? I think that they are a model for a public-private partnership in terms of relationship. I was fascinated at the amount of information that they started providing us once we got into that pool of people, if you will, or industries that they support.

NCSD provides a lot of information to us daily. Could it always be better? Nothing is ever perfect. I believe that every day they improve it. So I think they know it could be better and they constantly strive to do that.

Mr. MCCAUL. What needs to be done to engage the private sector more in this area? We heard from Mr. Turner that the private-sector security is not always where it should be. What needs to be done to really bring in the private sector more to make them more of a leader in this area?

Mr. SILVA. I am sure Mr. Turner will have something to say about this, but I will just say a couple of words on that. I think as long as it is viewed as a partnership, and you are not asking the private sector to just come in and sort of donate a bunch of effort and a bunch of time, and all of a sudden deep dark secrets wind up in the press. I think some of the issues have been addressed with respect to what information could be retrieved from FOIA, with information sharing. I think that was a big step in the right direction. We have seen a lot of positive movement because of that.

So I think the biggest thing is to approach it as a partnership. It is a give and take. The good news is that I think that NCSD has taken their relationship with the private sector, they bring that information together; they sort of sanitize it, anonymize it, if you will, and then they can produce a cohesive report. Literally every day, they produce a daily summary of what the situation is.

Mr. MCCAUL. So the FOIA exception that was passed that would protect your reporting a vulnerability, which obviously a private company is not going to want to report that for obvious reasons—shareholders and stock price. That has helped in the information sharing process with the government, in your view.

Mr. SILVA. It absolutely has. In fact, if you break this down a little bit, Mr. Dixon cited earlier that there were a number of vulnerabilities and incidents that had been reported, and it was tens of thousands. It is a big number. Bear in mind that that num-

ber is only from the people who have willingly reported it, and I dare say that the number is significantly higher that goes unreported.

Mr. MCCAUL. Mr. Turner, you said something that caught my attention. You said that experts have found that all the systems suffer from high-impact security vulnerabilities that could be exploited by a low skill-level attacker. We always hear the story about the teenager learning how to hack into a computer network system and crash it, and then we think about that kind of capacity, that sort of skill on the part of a criminal or in the worst-case scenario, a terrorist.

Yet, that is what you are reporting the experts have found. How do we strengthen that system so low skill-level, which would include obviously not a whole lot of knowledge to do it. How do we greater protect the system?

Mr. TURNER. As I mentioned previously, the best way to approach this is holistically, meaning that you have to motivate the vendors to start including better security controls in the base technologies themselves. And then you also have to make sure that the infrastructure owners are properly trained to architect those systems properly so they don't defeat the security controls that the vendor develops.

And so in the case that further on in the testimony you will notice, some of the existing systems cannot necessarily be retrofitted with security technologies or enhanced security controls, while still maintaining system reliability. So that is going to be the barrier to entry for improve security for these private infrastructure owners. They are going to be the ones who have to make that decision of when do we rip and replace; what is the pain threshold that we have to go through.

I think the role of government there is establishing this level playing field so that people understand these are the minimum standards, and then you defeat some of the market forces and the resource constraints that these private infrastructure owners are apparently under. So it is a combination of government motivating the private infrastructure owners to make the investment; informing the technology vendors about how to go about improving the technology; and then informing the infrastructure owners how to deploy it properly. I think that is the three-phase approach.

Mr. MCCAUL. Do you agree with that, Mr. Silva, from the private-sector standpoint?

Mr. SILVA. Yes, I do. I think that certainly incentives, whether positive or negative, definitely have an impact on that sort of thing. In terms of the vendors actually incorporating security into their software or their products, there is a huge challenge in that it still has to be usable, okay?

So BlackBerrys, for example, are a very useful tool and a lot of people use them, but not a lot of people want to have to enter a password every time that they want to check their e-mail on that. So what happens is that they frequently turn it off, making it far less secure if you leave that on an airplane, and someone picks it up, and they basically have your whole mailbox.

So there is a tradeoff between usability and security. Unfortunately, oftentimes, things that are more convenient are often less secure because of that.

Mr. MCCAUL. If I can just throw one last one, in terms of when we are talking about vulnerabilities—and if you can't give me a specific percentage breakdown, I understand—but how much are we vulnerable because of technology weaknesses in the system, versus just what you talked about, and that is, for lack of a better term, operator error?

Mr. SILVA. Oftentimes, the biggest vulnerability in any network sits between the keyboard and the back of the chair. So what will frequently happen is that users will make the system more accessible for themselves, their children, their coworkers, you know, what have you. And by and large, and the thing we have not really talked about here today is the insider threat, not just outsider threats, but insider threats.

In fact, most of the most serious penetrations in networks have actually occurred from inside the network, where people actually steal the money or steal intellectual property from inside the company. But oftentimes, people will do things for their own convenience which inherently make the system less secure.

Mr. TURNER. And we would back that up with the findings that we have had in our assessments. You can make the best, most secure technology, but if it is inconvenient in the end-users perspective, it often gets disabled. So it is an awareness issue all the way through to the end-user.

Mr. MCCAUL. Thank you. I see my time has expired.

Mr. LANGEVIN. I thank the gentleman.

The gentleman from California, Mr. Lungren, is recognized for 5 minutes.

Mr. LUNGREN. I thank the gentleman.

I thank the gentleman from Texas for leaving me some time. I appreciate this.

[Laughter.]

Mr. MCCAUL. I was trying to filibuster.

[Laughter.]

Mr. LUNGREN. Mr. Chairman, I would just like to suggest if we are going to conduct hearings on these high-technology issues here, we might ask if they could at least get the two clocks to be coordinated.

[Laughter.]

According to one, it is 8 minutes to 10:00, and the other one says it is 7 minutes after 7:00.

Mr. LANGEVIN. I would check my BlackBerry, but I don't know if that is working right now.

[Laughter.]

Mr. LUNGREN. Well, for security reasons, no one knows what time it is.

Here is the question. In the private sector, how do we make them do more than they are doing now, because you are talking about these control systems that are controlling more and more. How do we get them to understand better that security of this nature is acceptable to their bottom line? In other words, if I sell a product, my bottom line is expressed in some ways by the more attractive

I make my product. So the user sees air conditioning in the car; sees a new transmission, those sorts of things.

Here you are selling products to individuals who want to make it user-friendly, want to make sure it works, but embedded in that is the threat against security. Therefore, embedded in that has to be the security against that invasion. How do we make it real for a CEO to listen to his I.T. security guy, the man or woman who comes in and says, there is this vulnerability, but—and I am quoting you, Mr. Silva—there are all kinds of vulnerabilities out there. There are attacks going on every day. Everybody sort of has them.

How do I improve my product—and of course, we are talking about critical infrastructure—how do I improve it so that I can show my bottom line to my shareholders, to the taxpayers, to whoever, when perhaps the possibility of a catastrophic event is very small, but the consequence is huge. How do we do that when it is hidden the way it is, as you suggested?

Mr. TURNER. The first approach that you have to look at this is you are exactly right. In a true risk management equation, without threat, without some sort of over-act, or some sort of large incident, it is very tough to drive purely business-focused people, because they can't manage an unknown threat. You can talk about the worst impact in the world, but until there is some sort of incident, most times the people who are in pure risk management situations will not take any action.

So with that sort of backdrop, you have to move into a situation where the people who manage the business of providing critical infrastructure are educated for the vulnerabilities that exist in their systems. In many cases, they don't understand. Now, that education is where we have been spending a lot of effort, reaching out to industry at INL to help educate folks, but still there is a long ways to go.

Mr. LUNGREN. So the government could do a lot in terms of education. I think that is an obligation.

The next question is, what do we do in terms of regulation? If we do regulation, what is the nature of that regulation? Because if we do try and articulate what the range of fixes are, as you suggest, before the ink is dry, that may not be the right fix.

So what is the—if you have any suggestions for us—the parameters of our legislative action that would create the incentives for this kind of protection you are talking about, on the one hand, and not diminish the ingenuity of the private sector, where they might find a fix that we haven't even thought about, but they are doing that job.

I know that is a general question, but that is really the tough thing that we have here.

Mr. SILVA. It is a very fair question. Some of this was sort of addressed. Some examples of what you are talking about are things like the SAFETY Act, for example, where if you meet a minimum set of standards, you know your liability is limited, those sorts of things. There has to be some form of an incentive to get the average company to participate in an aggressive security activity.

Some examples where we have seen some improvement have been around Sarbanes–Oxley, okay? So Section 404 of that sort of

suggests some security measures which need to be taken, and the board holds them accountable. But when a CSO walks into the CEO's office and says, boss, I need $100 million to enhance the infrastructure because it might go down for 1 hour in the next 3 years, okay? If I were a bank, I might accept that risk and say it is not worth $100 million to me. I can afford to be down 3 hours in the next 3 years.

At VeriSign, we don't have that luxury, because if we go down, every enterprise is down for 3 hours, and that is not a luxury we have. So I am fortunate as a CSO in that my CEO gets it, but I don't think that you can make business sense to most CEOs that you want to spend tens or hundreds of millions of dollars fortifying an infrastructure with no financial return on it. So that is the challenge.

Now, what Congress can do in particular is if you want strengthened software and better products, then insist on it when you buy them.

Mr. LUNGREN. So we will spend more money.

Mr. SILVA. You are already spending the money, right? You are already spending the money. You decide who you are going to spend it with based on the capabilities that they offer. This is not unprecedented. It has happened in the past.

Mr. TURNER. To back up his comments, I think what is important is that if you are looking to take action, the first thing you can do is help to dedicate folks towards specific aspects of the area, so there is no one-size-fits-all security mechanism. Help the private folks categorize and prioritize their assets that support critical infrastructure, and then help them, motivate them to whatever mechanism you deem most appropriate to move towards something that is more proactive from the security perspective.

Mr. LANGEVIN. The time has expired.

I want to thank the witnesses for their very valuable testimony and the members for their questions.

This is not the last hearing that we hold on cybersecurity, I can promise you that. I look forward to working with you as we go forward. The issue is too important to ignore.

Again, we thank you for your testimony here today.

The members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously to those questions.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 3:56 p.m., the subcommittee was adjourned.]

APPENDIX A

PREPARED STATEMENTS

PREPARED STATEMENT OF THE HONORALBLE JAMES LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE, AND TECHNOLOGY

• Ladies and gentlemen, welcome to the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology hearing on the hacking of federal systems and privately-owned critical infrastructure.
• I'd like to begin by thanking the witnesses who appear before us today, and I appreciate your testimony.
• I'd like to focus my remarks this afternoon on our first panel, which will discuss the security of information technology on the federal level.
• Let me be clear about the threat to our federal systems: *I believe that the infiltration by foreign nationals of federal government networks is one of the most critical issues confronting our nation.*
• The acquisition of our government's information by outsiders undermines our strength as a nation. If our sensitive information is stolen and absorbed by our enemies, we are strategically harmed.
• **Over time, the theft of critical information from government servers could cost the United States our advantage over our adversaries. This is a most critical issue that we cannot afford to ignore any longer.**
• Today we're hearing from several agencies that have experienced significant cyber attacks against their systems.
• These are not the only agencies experiencing these problems. They are simply the only attacks that have been made public.
• In October 2006, hackers operating through Chinese Internet servers launched an attack on the computer system of the Bureau of Industry and Security (BIS) at the Department of Commerce.
• The hackers penetrated the computers with a "rootkit" program, a form of software that allows attackers to mask their presence and then gain privileged access to the computer system.
• In reviewing the Commerce testimony for today's hearing, I am troubled by several things.
• Though Commerce learned on July 13 that its computers were first infected, this was *not* the date of initial infection. **In fact, Commerce has no idea how long the attackers were inside their systems, nor do they know if the attackers *are still within their systems.*** As far as I can tell from the responses, rogue tunnel audits, authentication changes, and complete machine rebuilds have not occurred.
• We're also not sure how much information was lost. Though Commerce tells us that data was not "lost," data can easily be "copied" and sent outside through the Internet.
• Unfortunately, Commerce isn't the only federal agency with a problem.
• Prior to the Commerce hack, in June 2006, hackers accessed networks at several State Department locations, including its Washington headquarters, and inside the Bureau of East Asian and Pacific Affairs.
• They did so by sending a socially-engineered email to an employee. The employee opened the Microsoft Word document attachment, which contained an exploit code.
• I am concerned about the temporary fix that State put in place.
• Security authorities that I have spoken with are highly dubious about the success of "temporary wrappers," the kind which State had to put in place due to the absence of a Microsoft patch for several months.

• Most targeted attacks involve root-kits, which cannot be detected or stopped by a "temporary wrapper." I don't understand, therefore, why State wouldn't take its entire system offline for a full kernel inspection.
• In reading State's testimony, I believe that State made the determination that ***accessibility to data*** is more important than ***confidentiality and integrity.*** If State really valued confidentiality and integrity, they would have taken the system off line and done a full wash.
• Both agencies insist that these attacks are less serious because they involve "unclassified servers." I disagree.
• As you are no doubt aware, FISMA requires federal agencies to track down and identify every device and system on an agency's network, and to make sure that the network topology is fully described.
• As we learned last week, both State and Commerce received F's in the latest round of FISMA scores. According to page 10 of the Fiscal year 2006 FISMA Report to Congress, the Inspector General at the Department of State reported that the agency did not complete at least 50% of its system inventory. The IG at the Department of Commerce certifies that at least 96% of Commerce systems have been inventoried.
• I will suggest to our panelists today that if they can't certify their network topologies to FISMA, then they can't know for certain whether these incidents don't involve the classified networks.
• Furthermore, just because these attacks are occurring on the unclassified network does not mean this isn't sensitive information. Information that may be deemed "classified" in the future may first appear on an unclassified network.
• But this isn't just about Commerce and State.
• **I am disappointed and troubled with the Department of Homeland Security's progress in securing cyberspace.**
• The Department is the agency responsible for securing the nation's critical infrastructure, and yet they received a "D" this year on its FISMA score. It is the first time since 2003 that the Department did not receive an "F."
• Our issue today is with the NCSD, but I'll be honest with you: I don't know how the Department thinks it's going to lead this nation in securing cyberspace when it can't even secure its own networks.
• Not only are these grades embarrassing, it's dangerous. Think about all of the critical information the Department is keeping on its networks. I can assure everyone here that the kinds of questions that have been asked to the State Department and the Commerce Department will be asked to DHS.
• With regard to NCSD's response to these incidents, I have a few thoughts.
• It is my understanding that NCSD does not adequately share commonalities of attack information with other agencies that may be at risk. For instance, an agency like Commerce or State that has been hacked by a "zero-day exploit" will provide this information to the NCSD. But the NCSD can't just sit on that information.
• We need the NCSD to be the group that fuses information from across the federal government together and distributes a product for agencies to use.
• Unfortunately, I understand that NCSD does not have protocols in place to share this kind information with other agencies in the federal government or perform that level of work.
• This subcommittee will continue to monitor these issues to ensure that information sharing and technical response improves.
• In closing, I think these incidents have opened up a lot of eyes in the halls of Congress.
• We don't know the scope of our networks. We don't know who's inside our networks. We don't know what information has been stolen.
• We need to get serious about this threat to our national security.

PREPARED OPENING STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

• I want to thank Chairman Langevin for holding this critical hearing.
• I've been tracking this issue for some time now.
• In October 2006, when the world first learned of the hacking incident at the Department of Commerce, I sent a letter to the Assistant Secretary for Cybersecurity, Greg Garcia, asking several specific questions about the role of the Department in responding to this incident.
• Unfortunately, I never received a response back from the Department.
• I understand that I'm not the only one being left in the dark when it comes to the Department's efforts in cybersecurity.

• If I understand Chairman Langevin correctly, many federal agencies are waiting for the Department to provide them with timely intelligence and recommendations about hacking incidents at the federal level.
• Many in the private sector are also telling me that the Department is failing to provide the guidance and partnership necessary to successfully secure cyberspace.
• It is clear that our government, working together with the private sector and academia, must do more to ensure that cybersecurity is a priority in our nation(s homeland security strategy.
• In 1996, the United States government undertook the first national effort to secure our networks.
• Unfortunately, I don't believe that we are any further along today in our efforts to secure cyberspace.
• Programs and initiatives that were developed over the past ten years have been dismantled and, in certain instances, are just now being re-created by the government.
• We can see that this Administration views its priorities in cyberspace differently from the last Administration.
• The most senior ranking official within the Administration exclusively responsible for cybersecurity has gone from being a Senior Advisor to the President to an Assistant Secretary position buried several layers down in the Department of Homeland Security bureaucracy.
• I'm glad to read in Mr. Dixon's statement that "coordinating better cyber security practices across the Federal government" is one of Secretary Chertoff's "highest priorities."
• But this rings hollow to me when I think about how long it took him to appoint an Assistant Secretary for Cybersecurity.
• I also wonder why the Secretary believes that this Department will be able to coordinate better cyber security practices across the Federal government, when his own Chief Information Officer just received up a "D" in the recent FISMA grades.
• Finally, I'm wondering why the Secretary wouldn't send Mr. Garcia up on this first panel to testify. I can think of no better opportunity for him to work on coordinating better cyber security practices across the Federal government than sitting next to the State and Commerce Departments at this hearing.
• I look forward to hearing the testimony and I appreciate the witnesses for being here today.

APPENDIX B

ADDITIONAL QUESTIONS AND RESPONSES

QUESTIONS FROM THE HONORABLE JAMES. R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE, AND TECHNOLOGY

RESPONSES FROM JERRY DIXON

Question 1.: What kinds of products does the Department provide to other agencies when the Department hears about a "zero day" exploit? Does the Department send intelligence products to other agencies suggesting ways that they can remedy the vulnerability? Does the Department send patches that agencies can install on their own systems?

Response: ***Zero-Day Exploits***

A zero-day exploit is one that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both the exploit and vulnerability makes it extremely difficult to defend against. In many cases, the critical nature of the exploit puts the vendor in the spotlight with the pressure to create a fix as soon as possible.

Defending against zero-days is a difficult task for even the most vigilant administrator or experienced computer user. Establishing and following best practices is still the best defense in network security. These practices will help organizations decrease risks and determine incident response procedures should a need occur.

US–CERT Vulnerability Disclosure Policy

To support its operational mission, the United States Computer Emergency Readiness Team (US–CERT) focuses its programs and initiatives on enhancing situational awareness, increasing collaboration across Federal operational security teams, preventing or quickly containing cyber incidents, and providing for inter-agency coordination during a cyber event. US-CERT established a vulnerability remediation process and a national alert system in order to collect, mitigate, and disseminate vulnerability information to Federal, public, and private partners.

Vulnerabilities reported to US–CERT are forwarded to the affected vendors as soon as practical after the report is received. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. US–CERT's goal is to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of a publication schedule is based on the best interests of the overall community.

US–CERT provides Federal agencies and the public with actionable information regarding zero-day exploits in the form of technical and non-technical cyber alerts. These products are posted on the US–CERT public website, as well as distributed through the National Cyber Alert System. Federal agencies receive this information at the same time it is disclosed to the public.

The cyber alerts contain recommendations and work-around for risk mitigation. After coordinating with vendors and gathering as much technical and threat information as possible, US–CERT takes steps to notify end users about the vulnerability. US–CERT strives to disclose accurate, neutral, objective information focused on technical remediation and mitigation. Targeting a technical audience (system administrators or others who are responsible for securing and patching systems), the alert describes the vulnerability in some detail, providing sufficient information for the user to make an informed decision about the risk. US–CERT will reference other available information and correct misinformation when possible.

US–CERT provides patch information and links for patches that can be downloaded as soon as they are available from the vendor. US–CERT does not create, nor does it endorse the use of third-party patches, for they are considered "buyer-beware" and could introduce new problems or unforeseen configuration issues. Instead, US–CERT recommends that all organizations consider their options carefully and work with the vendor when faced with a zero-day threat.

Question 2: What is the role of Assistant Secretary Garcia in the FISMA process?

Response: The Federal Information Systems Management Act (FISMA) directs OMB to maintain a Federal information security incident center to perform the following functions: 1) provide timely technical assistance to agency information system operators; 2) compile and analyze incidents that threaten information security; 3) inform agency information system operators about current and potential information security threats and vulnerabilities; and 4) consult with the National Institute of Standards and Technology (NIST), agencies or offices operating or exercising control over national security systems. It also requires all Federal civilian agencies to implement FISMA and to ensure the operation of a central Federal information security incident center. Although FISMA assigns this function to OMB, the Director of OMB has, in turn, issued guidance to Federal departments and agencies stating that DHS' US-CERT performs these responsibilities, which is under the leadership of Assistant Secretary Garcia.1

FISMA requires all Federal civilian agencies to notify the National Cyber Security Division (NCSD)/US–CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information (PII) within one hour of discovery. US–CERT collects this information to identify trends and provides regular reports to OMB. NCSD is promoting the need for Federal agencies to commit adequate resources to strengthen their networks, and to utilize robust technology security requirements in the procurement process combined with reasonable security practices.

Question 3: In your experience, what percentage of governmental network security weaknesses are technology based and what percentage is based upon the failure to follow necessary protocols and procedures? In other words how many weaknesses are based on a lack of the proper security tool and which are based on network operator error?

Response: All Federal agencies face ongoing challenges to maintain the security of their systems, which include both addressing security weaknesses and ensuring that processes and procedures are in place and followed to maintain security.

Based on the experience of NCSD/US–CERT, the two greatest weaknesses in Federal government networks stem from the inherent vulnerabilities in operating systems, application software, and/or protocols, as well as the lack of user training/education. New exploits for vulnerable technology are discovered, targeted and exploited on a daily basis. In addition, end users are many times the greatest weakness, as they continually open unsolicited e-mail, respond to unsolicited e-mail, are sometimes targeted by e-mail, and visit malicious websites that can lead to intrusions.

The NCSD/US–CERT maintains a number of programs and initiatives that focus on increasing security across the Federal government, which serve to address security weaknesses, improve awareness about good security practices, enhance coordination during a cyber event, and increase collaboration among Federal operational security teams. An example of this is the Government Forum of Incident Response and Security Teams, which is comprised of over 400 members from Federal Operational Security Teams, Chief Information Security Officers, and information security policy makers. In addition, the National Cyber Response Coordination Group (NCRCG) comes together for National Response Plan implementation or incident coordination. The NCRCG is comprised of cyber security experts from all of the cabinet departments, and facilitates inter-agency coordination activities in response to major cyber incidents affecting the public or private sector.

○

VerDate Nov 24 2008 07:50 Jun 15, 2009 Jkt 000000 PO 00000 Frm 00073 Fmt 6601 Sfmt 6011 H:\DOCS\110-HRGS\110-26\43562.TXT HSEC PsN: DIANE