CYBERSECURITY: EMERGING THREATS, VULNERABILITIES, AND CHALLENGES IN SECURING FEDERAL INFORMATION SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MAY 5, 2009

Serial No. 111–51

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE
56–581 PDF WASHINGTON : 2010

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 OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio
——— ———

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

DIANE E. WATSON, California, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
HENRY CUELLAR, Texas
JACKIE SPEIER, California
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
MIKE QUIGLEY, Illinois

BRIAN P. BILBRAY, California
AARON SCHOCK, Illinois
JOHN J. DUNCAN, JR., Tennessee
JEFF FLAKE, Arizona
——— ———

CONTENTS

CYBERSECURITY: EMERGING THREATS, VULNERABILITIES, AND CHALLENGES IN SECURING FEDERAL INFORMATION SYSTEMS

TUESDAY, MAY 5, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Diane E. Watson (chairwoman of the subcommittee) presiding.

Present: Representatives Watson, Connolly, Cuellar, Bilbray, and Issa [ex officio].

Staff present: Bert Hammond, staff director; Valerie Van Buren, clerk, Adam Bordes, professional staff; Adam Fromm, minority chief clerk and Member liaison; Dr. Christopher Bright, minority senior professional staff; and Molly Boyl and John Ohly, minority professional staff.

Ms. WATSON. The committee will now come to order. Today's hearing will examine the Federal Government's efforts to secure its networks and cyber-based critical infrastructure assets. We will also look at the changing threat and vulnerability landscape against Federal networks and how legislation to counter these elements oughtto be crafted.

Without objection, the Chair and the ranking minority member will have 5 minutes to make opening statements followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition.

Without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

I want to welcome our witnesses and I want to welcome the Members who are here. This hearing on threats, vulnerabilities, and challenges in securing the Federal Government's information systems and infrastructure is very necessary and very important. Our distinguished witnesses are here; we look forward to your testimony.

I will preface my remarks by stating that today's hearing is only the beginning of our efforts in this Congress to strengthen the Federal Government's information security posture. I know many of my subcommittee colleagues, including Ranking Member Bilbray, recognize the critical national security issues associated with cyberattacks from both domestic and foreign sources. I look forward to working with them in developing legislation this session to counter these threats.

Furthermore, I want to express my disappointment that DHS will not be providing a member of its new senior leadership to testify before us today. With all of the proposals under consideration in Congress for improving our cybersecurity posture, I think today was a missed opportunity for the Protection and Programs Directorate to explain the value they bring to the table. It is my sincere hope that they will become more engaging with this subcommittee as we move forward on these issues.

According to the Director of National Intelligence's 2009 Threat Assessment, the cybersecurity threat landscape continues to expand as the number of actors using cyberspace for attacking and disrupting our Federal critical infrastructure proliferate. These actors include foreign governments, terrorist organizations, individuals with nefarious motives, and plain old-fashioned criminal syndicates looking to use cyberspace as a tool for compromising Federal networks and Government operations.

Cyberattacks against Government networks are nothing new, but their complexity and disruptive capabilities have increased significantly in recent years. In the past few weeks alone, we have become aware of reported breeches to critical DOD programs such as the Joint Strike Fighter and Marine One Presidential Helicopter, as well as to the Air Force's air traffic control system. Congress has also been the target of cyberattacks originating from the People's Republic of China on numerous occasions dating back to 2006. These episodes are a threat to our national security interests and our ability to conduct Government business without disruption.

Complicating matters are advances in technology that enable cyber-criminals of all stripes to remain ahead of Federal information security efforts. As new commercial IT products and services become more widely available, such as wireless networks and devices, file sharing applications or peer-to-peer software, and new services like cloud computing, we often fail to incorporate effective security controls to correspond with their use.

A significant focus of today's hearing is our lack of a harmonized framework for organizing and coordinating Government-wide information security policies and practices. Although there are many reasons for this, I will mention some that come to my mind: To begin, we currently have too many cooks in the kitchen. The OMB, DHS, and DOD all have a major role in the security of our information infrastructure. Furthermore, DHS has thus far failed miserably in its charge to manage cyber-response and coordination efforts for Federal agency stockholders through duplicativee, overlapping divisions within the Protection and Programs Directorate. Last, it remains unclear how efforts under the administration's mostly classified Comprehensive National Cybersecurity Initiative are aligned with current statutory and regulatory requirements for both civilian and military networks. Until there are uniform principles, policies, and requirements established for all agencies, I fear that our patchwork approach to cybersecurity will have a minimal effect in securing our information infrastructure.

Over the past decade, the Federal Government has made significant progress in the area of information security. Laws such as the Federal Information Security Management Act have forced agencies to recognize the need for stronger physical, technical, and administrative safeguards for IT assets in order to counter the ever-increasing number of threats in cyberspace. Nevertheless, such policies have only scratched the surface for determining what our real cyber vulnerabilities are. More importantly, these efforts have done nothing to ensure that Government contractors who operate systems on an agency's behalf have adequate security measures in place. To me, this is unacceptable and must be addressed in any future legislative proposals.

In summary, I hope our witnesses will provide us with a comprehensive, high level assessment of our current posture and capabilities for adjusting to new cyber-based threats and vulnerabilities. I would also welcome your recommendations for legislative principles that would promote a more harmonized and uniform approach to cybersecurity across the Government's systems.

Once again, I thank our panelists for joining us today. I look forward to your testimony.

I now recognize our ranking member, Mr. Bilbray.

Mr. BILBRAY. Thank you, Madam Chair. Madam Chair, first of all I would like to introduce for the record a written opening statement, please.

Ms. WATSON. Without objection.

Mr. BILBRAY. Thank you. Madam Chair, I want to thank you for having this hearing.

It is sad that DHS had to cancel out on Friday because I think this is one of those real critical elements where there can be not just bipartisan cooperation in this body but coequal cooperation with the executive branch to address this issue.

I just hope that we all recognize we are having a hearing today and remember that when the 9/11 Commission came down about how 9/11 could happen, it was because the Federal Government did not go back and reevaluate structures and firewalls that had been created from the Watergate period. And it really didn't think it was important enough to be bothered with reinvestigating what could have happened here.

I think what we need to recognize is, if we are old enough to remember the Y2K fear, the impact of a Y2K created, designed, and executed with intent. That is just the tip of the iceberg of what we could face.

Madam Chair, I want to thank you for having this hearing, and having it with or without the Department of Homeland Security. I think that we need the discussion now and early to make sure our procedures are in a manner that faces the new threats rather than trying to fight the battles of the past. I hope that you and I can work together to make sure that we do not find ourselves where we were with 9/11 and saying, doggonit, why didn't we take care of this when we had a chance.

I am very proud to work with you and with the other Members here to make sure we can look back and say, thank God we did the right thing when we had a chance and time to do it. I appreciate the chance and being able to participate with you in this.

Ms. WATSON. I would like now to call on Mr. Connolly for his opening statement.

Mr. CONNOLLY. Thank you, Madam Chairman. Thank you so much for holding this important hearing. The number of incidents in which hackers have broken into Government files and systems, it seems to me, should impel Congress and the administration to take all possible steps to secure our systems.

The permeability of our systems is a risk not only to our national security but the future of our economic competitiveness as well. The ability of hackers to gain access to information from private companies about recent innovations reduces the potential for new economic growth and the incentive to innovate.

We are fortunate to be working with an administration that is tackling the problem aggressively by reviewing current cybersecurity policy and preparing potential reforms.

The testimony we are going to hear today paints a grim picture of the current state of cybersecurity but also suggests that there are some security steps that can be taken quickly and relatively easily. Mr. Sachs notes that 90 percent of security breeches addressed in a recent report were actually easily preventable. And according to Mr. Lewis, only one third of affected agencies have complied with Homeland Security Policy Directive No. 12, which suggested using secure network credentialing for employees.

By the way, something that underscores your point, Madam Chairman, and that of Mr. Bilbray is that it is too bad that DHS is not here today. My guess is that legislation is going to come out of this committee on the subject and DHS needs to be at the table. This committee has an important role, obviously, in identifying immediate steps the Federal Government can take to enhance cybersecurity.

The committee will also hear testimony from Mr. Lewis, who has stated that, "It is possible that the Internet as it is currently architected can never be secure." That is a pretty provocative statement, if true. From the statement, one would infer that a separate Internet-type system for Government usage will ultimately be necessary. That is an equally provocative conclusion. I look forward to hearing from all of the witnesses about whether the creation of a whole separate system is indeed a practical or efficient way to achieve cybersecurity, or if it is necessary.

Again, I want to thank you, Madam Chairman, for holding this hearing. I look forward to working with my colleagues and the administration to enhance cybersecurity by building upon what we learn from today's critical hearing.

Ms. WATSON. I now yield to Mr. Issa.

Mr. ISSA. Thank you, Madam Chair. As we hear today, the problems of cybersecurity continue to be vexing. We are going to continue to see these kinds of shortfalls.

What this committee uniquely has a role of looking at is the Government in its broadest sense. So hopefully today as we go through both the hearing and the questions that follow, we will begin asking the tougher questions.

First of all, is there any reason to be throwing the kinds of dollars spread over the entire Government as we did in the Supplemental in the Cybersecurity Initiative without demanding fixed results? Many of the dollars that have been spent under the previous administration and continue to be spent under this administration are essentially for upgrades. These can be completely bypassed if the Department of Defense's Secretary of Defense fails to have his own staff adhere to procedures for security as has previously been reported in the press.

Additionally, the gentleman made a good point: Do we need a separate Internet? Certainly, supernet and other theoretically closed systems have been penetrated by those same failures like the use of USB key fobs and the failure to lock down disk drives, floppy disks, and other devices that allow for penetration around, if you will, a closed system.

I am most concerned to hear that even our newest aircraft design was penetrated, in a sense, on a system that was designed to be closed. These and other failures show us that the money we have thrown at the problem, although spent, was mostly spent for the same business as usual Maginot Line that failed to protect France from the Germans and fails to protect us from hackers on the Internet.

Madam Chair, when we spend the kinds of tens of billions of dollars both in the classified and unclassified world, we do so with good intention. But if we do not begin working smarter, using techniques to attack our enemies, getting to the hacker before the hacker gets to us, changing or at least attempting to change international law so that it will allow us to consider acts by the Chinese and other less openly hostile governments as aggressive acts of cyberwar, then we do not and will not have the kind of peace we want.

Madam Chair, during my tenure on the Select Committee on Intelligence, as I saw one after another failure to secure the Department of Defense and other agencies no matter how much we hardened, I became convinced that in fact we talk about cybersecurity as though it is appropriately international espionage, international crime and yet we do not deal with it in a way that is appropriate. We do not in a hostile way routinely shut down the hackers, whether they are in Venezuela, China, or 100 other countries around the world. As a matter of fact, it is considered to be bad form for us to retaliate to somebody even as they hack into the House of Representatives.

So Madam Chair, I would hope that our questioning will go beyond how we can throw money at the problem and whether in fact we need international conventions and a will to deal with people who come through the Internet and attempt to hack us in a way in which the response is as punitive to them in a nonviolent but equally effective way as any other act of war. With that, I yield back.

Ms. WATSON. Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair. Thank you for having this meeting. As we look at the challenges in securing Federal information systems, I think, Madam Chair, that it is important that the Congress and the executive branch work together to develop this blueprint to protect our Federal information. One of the things is to have hearings like this where we can have the Department of Defense, the State Department, and other folks sit down.

But to have one of the agencies that is in charge of protecting our homeland, the Department of Homeland Security—and I am one of the chairmen of one of the subcommittees in Homeland—I am a little disappointed that they are not here. Apparently, my understanding was that you all gave them 3 or 4 weeks advance notice to be here and I guess they just canceled this last Friday. What was the rationale about that? If I may inquire of the chairwoman, what was the rationale for them not being here?

Ms. WATSON. We couldn't get the Director and the next person in line had a family emergency. We sought someone else at the upper levels but they could not attend. We are going to work on that so they will be in attendance at future hearings.

Mr. CUELLAR. Do we have anybody from the congressional liaison from Homeland Security present here today? I am sure we have somebody here.

Ms. WATSON. Apparently not. Nobody is jumping to put their hand up. So we will just assume.

Mr. CUELLAR. We will assume there is nobody here. Well, again, I can understand a family reason, but I do understand that there are other folks who can come here.

I do want to mention that I am a big supporter of Homeland Security but they do have a record of missing over 120 congressional mandates that we have set for them. I have spoken to the new Secretary and she assures me that they are going to work on deadlines and all that. But I think showing up is probably the first step to show a little cooperation with the Congress.

I hope there is another time when we can bring him here. I am sure we can set up something where if somebody can't come in, I am sure the second or the third person can come in. Because we are losing an opportunity.

The folks who are here today spent a lot of time to be here, a lot of time preparing. I know it doesn't mean that they just show up. It is a lot of hours in preparing to be here. It would have been nice if we would have had Homeland here so we can get a perspective from the Department of Defense, the State Department, and Homeland. We are losing an opportunity.

But Madam Chair, I look forward to working with you and the other members of the committee.

Ms. WATSON. I think as they get their footing they will cooperate with our committee. We will assure Members and the public that they will be part of this. We cannot continue to assess the information given, and maybe we will have to have a classified session with them, but for sure we will seek their input and their participation. I know they will cooperate. We will guarantee you that.

All right, if there are no further opening statements, we will now turn to our first panel. It is a policy of this Committee on Oversight and Government Reform to swear all witnesses before they testify. I would like to ask you both to please stand and raise your right hands.

[Witnesses sworn.]

Ms. WATSON. Let the record reflect that the witnesses answered in the affirmative. Thank you. I will now introduce our panelists.

The first is Mr. Robert F. Lentz, the Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance at the

Department of Defense. Since November 2000, he has been the Chief Information Assurance Officer for the Department of Defense and oversees a Defense-wide Information Assurance Cyber Program which plans, monitors, coordinates, and investigates IA cyber activities across DOD.

The other witness, Mr. Streufert, is the Deputy Chief Information Officer for Information Security at the Department of State. He is responsible for providing oversight and guidance for information assurance activities including security policy development, risk management, system authorization, training and awareness, compliance reporting, and performance measures. Prior to his tenure at State, he served in various IT management roles at USAID, USDA, and the U.S. Navy.

I ask that each of the witnesses give a brief summary of your testimony. Keep this summary under 5 minutes in duration if possible. Your complete written statement will be included in the hearing record.

Mr. Lentz, would you please proceed?

STATEMENTS OF ROBERT F. LENTZ, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER, IDENTITY, AND INFORMATION ASSURANCE, U.S. DEPARTMENT OF DEFENSE; AND JOHN STREUFERT, DEPUTY CHIEF INFORMATION OFFICER FOR INFORMATION SECURITY, BUREAU OF INFORMATION RESOURCE MANAGEMENT, U.S. DEPARTMENT OF STATE

STATEMENT OF ROBERT F. LENTZ

Mr. LENTZ. Good afternoon, Chairwoman Watson, Congressman Bilbray, and members of the subcommittee. I am pleased to appear before the subcommittee to discuss initiatives to enhance the Department's and the Nation's information assurance cybersecurity posture.

This is a critical priority for the Department of Defense. With information and information technology assets distributed over a vast enterprise with diverse domestic and international partners, we know that we cannot execute operations without the GIG, the Global Information Grid which is our DOD network. The GIG is where business goods and services are coordinated; where medical information resides; where intelligence data is fused; where weapons platforms are designed, built, and maintained; where commanders control forces; and where training, readiness, morale, and welfare are sustained.

Maintaining freedom of action in cyberspace is critical to the Department and to the Nation. Therefore, the Department is focused on building and operating the GIG as a joint global enterprise. This enterprise network approach coupled with skilled users, defenders, and first responders in partnership with the intelligence and Homeland Security communities will allow us to more readily identify and respond to cyberattacks.

The DOD Information Assurance Cybersecurity Program is thus aimed at ensuring that DOD missions and operations continue under any cyber situation or condition and that the cyber components of DOD weapons systems perform as expected. There are many examples of current initiatives in my statement for the record. I will quickly highlight a few this afternoon.

To protect sensitive data on mobile and portable devices like laptops, we help make discounted encryption products available to all Federal, State, local, and tribal government agencies and to NATO. Since July 2007, this program has resulted in a U.S. Government cost avoidance of approximately $98 million.

To address cybersecurity risks to the defense industrial base, we have put in place a multifaceted pilot for threat and vulnerability information sharing, incident reporting, and damage assessments.

For the global supply chain, the Department has launched a program to protect mission critical systems. This year, we are establishing four Centers of Excellence to support program executive offices and supply chain risk mitigation throughout the system lifecycle. Additionally, we are executing vulnerability assessments in accordance with the 2009 National Defense Appropriations Act.

We continue to rely on the National Centers of Academic Excellence in IA education for critical cybersecurity skills. There are currently 94 Centers in 38 States and in the District of Columbia. One of those Centers, as an example, the University of Nebraska at Omaha cosponsored and hosted last year's fifth annual cyber defense workshop.

In 2008, the Department helped bring cybersecurity to the Wounded Warrior Program. Wounded, disabled, and transitioning veterans are receiving no cost vocational training in digital forensics, a critical technical shortfall for the Nation and the Department. The program started out at Walter Reed and is now being expanded to other DOD and VA hospitals.

To further harden our networks against cyberattacks, the Department is implementing the Federal Desktop Core Configuration. This is a pivotal Government and industry cooperative venture starting with ubiquitous Microsoft products to make computers more stable and defensible.

In conclusion, the DOD CIO is working toward a resilient and defendable core network for the Department and for the Nation in the face of the daunting security challenges you talked about. We are preparing the GIG and the GIG-dependent missions to operate under duress and we are doing so under conditions of rising hostility. I am happy to take questions.

[The prepared statement of Mr. Lentz follows:]

RECORD VERSION

STATEMENT BY

MR. ROBERT F. LENTZ

DEPUTY ASSISTANT SECRETARY OF DEFENSE,

FOR CYBER, IDENTITY AND INFORMATION ASSURANCE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

SUBCOMMITTEE ON

MANAGEMENT, ORGANIZATION AND PROCUREMENT

May 5, 2009

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Good afternoon, Chairwoman Watson, Congressman Bilbray, and Members of the Management, Organization and Procurement Subcommittee. I am Robert Lentz, the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance representing the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. I am also the Department's Senior Information Assurance Officer. I am pleased to appear before the Subcommittee to discuss initiatives to enhance the Department's and the nation's information assurance/ cybersecurity posture.

Information assurance/cybersecurity (IA/CS) is a critical priority for the Department of Defense (DoD). With information and information technology (IT) assets distributed over a vast and wide-ranging enterprise and with diverse domestic and international partners actively participating in DoD missions, we know that we cannot execute operations without the Global Information Grid (GIG) – our DoD network. The GIG is not just a collection of individual networks that happen to share the same Internet access points; the GIG is how we operate; the GIG is where business goods and services are coordinated; where medical information resides; where intelligence data is fused; where weapons platforms are designed, built and maintained; where commanders plan operations and command and control forces; and where training, readiness, and morale and welfare are sustained.

Therefore, the Department is focused on building and operating the GIG as a joint global enterprise that can be depended on wherever we operate in the world and under any circumstances to include cyber attack. This enterprise network approach, coupled with skilled users, defenders, and first-responders and in partnership with the intelligence community, will allow us to more readily identify and respond to cyber attack – and still accomplish the mission.

The DoD cyber, identity and information assurance (CIIA) program is thus aimed at ensuring the following vision:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform as expected.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The Defense information environment securely and seamlessly extends to mission partners.

Strategic Goals

To realize this vision, the Department has established four strategic IA/CS goals:

Goal 1: Organize for unity of purpose and speed of action. This goal focuses on how IA/CS is considered as the Department plans for and evaluates use of cyber assets or the cyber domain in Defense missions, the development and sustainment of our IA/CS workforce, and the expansion of IA/CS capabilities and capacity through partnerships, whether they be intra-government, with academia, with information technology (IT) industries, with defense industries, or with our international and military coalition partners.

Goal 2: Enable mission-driven access to information and services. This goal addresses how the Department securely delivers the power of information to its warfighting, intelligence, and business communities.

Goal 3: Anticipate and prevent successful attacks on data and networks. This goal addresses how the Department configures and instruments the GIG with tools and technologies to prevent intrusions, detect intrusion attempts, and reduce attack surfaces to deny adversaries any opportunity or advantage.

Goal 4: Prepare for and operate through cyber degradation or attack. This goal addresses how the Department creates trust and confidence in its weapons systems, data, and networks; strengthens its IA/CS readiness; operates in a degraded cyber environment; and restores cyber capabilities.

These goals provide the means to protect and defend the GIG today and to improve IA/CS capabilities over time. We are progressing toward an enterprise information environment that can dynamically and automatically configure itself to counter any threat and facilitate any mission.

The Department has made significant advances toward the vision. We have:

- Joined forces with other federal agencies in a comprehensive national cybersecurity[1] initiative to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed a DoD Information Management/Information Technology (IM/IT) Strategic Plan to further transition to net-centric operations to achieve information advantage.
- Recognized cyberspace as a global domain within the information environment, developed a National Military Strategy for Cyberspace Operations (NMS-CO), embraced a Network Operations (NetOps) construct for operating and defending the GIG, and, under United States Strategic Command (USSTRATCOM), integrated NetOps with other cyber operations.
- Stood-up and connected key cyber centers such as the National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), and the Defense Cyber Crime Center (DC3) as well as certified all 25 network defense centers across DoD.
- Operationalized the Joint Task Force for Global Network Operations (JTF-GNO) under USSTRATCOM.
- With industry and academia, developed the IA Component of the GIG Integrated Architecture and plans and programs for delivering key identity and IA/CS capabilities as enterprise services.

[1] The U.S. Government currently defines *cybersecurity* as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (NSPD 54/HSPD 23).

- Partnered with the Director for National Intelligence (DNI) to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of all levels of classified/sensitive information and to protect sensitive or controlled unclassified information to include sharing with our closest partners.
- Established a cybersecurity program in partnership with the Defense Industrial Base (DIB) to protect unclassified information relevant to Defense-related research, development and procurement.
- Established DoD policy addressing the relationship between cyber offensive and defensive actions called Computer Network Defense Response Action (CND RA).
- Worked with the National Counterintelligence Executive (NCIX) and Insider Threat Advisory Group to foster collaboration on the use of insider threat IA/CS tools.
- Created a DoD Venture Catalyst Initiative called DeVenCI to aid in the invention of cutting edge IA/CS solutions.
- Developed a comprehensive IA/CS policy framework that ranges from identity protection to wireless and satellite security to workforce training and education.
- Created the National Cyber Response Coordination Group in partnership with the Departments of Homeland Security and Justice.
- Launched a comprehensive cryptographic modernization initiative.
- Established a trusted foundry program and sought ways to improve microelectronics and software assurance.

The breadth and depth of all the programs and initiatives underway within the Department is too large to cover here. However, I would like to highlight a few current enterprise initiatives within the DoD CIIA program, organized by our strategic goals.

Goal 1

In support of Goal 1 (Organize for unity of purpose and speed of action), I will highlight our efforts to establish a DoD cyber workforce, partner with the DIB in a cybersecurity pilot, and build an international IA program.

Workforce

While our long-term aim is to achieve robust machine-to-machine network defense capabilities, people will always remain our frontline against cyber adversaries. From the everyday user to cyber defenders, the DoD workforce needs to be fully trained and qualified in key areas, and appropriately deployed to leverage and protect the Department's tremendous investment in information and communications. Achieving a technically adept cyber-capable workforce is job one! Competency in multiple IA/CS skills along with extraordinary cyber expertise or "black belts" in specialty areas, plus joint exercises to foster greater knowledge throughout the cybersecurity community has become a core priority of the Department.

To this end, the Department is continuing to expand the range and quality of IA/CS training available to its workforce. The technical schools of the military services have expanded their IA/CS curricula to meet DoD common baseline training and certification requirements. For example, the Air Force's school at Maxwell, AL, and the Navy's program at Pensacola, FL, are offering tremendous new programs. The Defense Information Systems Agency (DISA) sponsored Carnegie Mellon Virtual Training Environment provides real-time, on-line interactive IA/CS technical training to both military and civilian workforce members wherever they are in the world. The Information Resource Management College (IRMC) at the National Defense University here in Washington, DC now offers an advanced IA/CS curriculum supporting baseline standards to both DoD and federal leaders in all Departments. The military service academies and post-graduate schools are also heightening focus on IA/CS. Recently, the Army, Navy, and Air Force academies competed in the ninth-annual cyber game for cyber warriors.

The Department has a rich suite of simulation and exercise tools analogous to flight simulators that create realistic and secure environments for training and practicing IA/CS skills. This approach provides opportunities to "see" and respond to threats in a controlled environment, and rapidly build skills and experience without disrupting operational networks.

The Department has also developed IA/CS awareness training to help users and leaders to better understand their roles in defending DoD networks. The 2009 DoD IA Awareness training product introduced a new more interactive approach to teaching end users about their critical role in securing our networks. Our compliance reports show that 2.1 million personnel successfully completed this user awareness training program. Leadership development curricula in the military service and Joint Professional Education Programs have increased emphasis on IA/CS awareness to improve operational leaders' understanding and support for CIIA requirements. Operational leadership support is critical for effective execution of IA/CS activities at all levels.

The National Centers of Academic Excellence in IA Education (CAE) are producing graduates with the right skills to achieve a world class cyber workforce that includes both defensive and offensive capabilities. The CAE and CAE-Research (CAE–R) programs reduce the vulnerability of our nation's information infrastructure by promoting IA higher education and research and by producing a growing number of professionals with IA expertise in various disciplines. Currently, there are 94 CAEs across 38 states and the District of Columbia, including five military academic institutions: the Air Force Institute of Technology, the IRMC, the US Military Academy at West Point, the Naval Post-Graduate School, and the US Air Force Academy. For many students, especially graduate students, research is their "true educational experience." We must continue to expose these students to our hardest problems. The aim of the CAE-R program is to advance IA technology, policy, and operations that enable the nation to effectively prevent or respond to catastrophic cyber events. The CAE-R designations total 23 IA research centers across 17 states and the District of Columbia.

The CAEs provide DoD with many partnering opportunities. One example is the *Wounded Warrior Training Program* for America's wounded, disabled, and transitioning veterans. Mississippi State University's Forensics Training Center, in collaboration with Auburn and Tuskegee Universities in Alabama, is providing no-cost vocational training to veterans in a critical technical shortage area – digital forensics. In the fall of 2008, the Department helped bring this training program to the Walter Reed Army Medical Center in Silver Spring, MD. The intent is to offer the program for recovering military personnel at other major hospitals across the country this year and beyond.

Currently the Department is evaluating partnerships with University of California, Davis and University of North Carolina, Charlotte for *secure software development education,* including secure coding clinics for students. The intent is for students to receive an in-depth introduction to secure software techniques, have access to the tools and methods used to fix software vulnerabilities, and understand how to use them. The partnership, if undertaken, would be a key step in providing critical and leading edge software engineering skills to students who are potential DoD or federal employees.

Defense Industrial Base

In early 2008, the Department initiated a DIB Cyber Security and Information Assurance (CS/IA) pilot program to address cybersecurity risks to DIB unclassified networks that support DoD programs. The DIB CS/IA pilot has five major components: a binding bilateral DoD-DIB company framework agreement to facilitate CS/IA cooperation; threat and vulnerability information sharing; DIB network incident reporting; damage assessments; and DoD acquisition and contracting changes, including proposed changes to Defense Federal Acquisition Regulation Supplement (DFARS). The DoD-DIB legal framework provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected.

Under this program, the Defense Cyber Crime Center (DC3) is the focal point for threat information sharing. DC3, in coordination with other cyber centers, analyzes and disseminates near real-time threat information. To further strengthen near real-time information sharing and collaboration between DoD and its DIB partners, DoD is developing a secure electronic data/voice communication network called DIBNet. The DC3 also performs digital forensic analysis on reported DIB intrusion sets. These processes are labor intensive and require resources and advanced skills.

The Damage Assessment Management Office in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics orchestrates our military service damage assessment cells and is helping to standardize methodologies. Through damage assessments, the Department will be able to better determine the extent of compromised DoD information, as well as assess the overall impact of the compromise on current and future weapons programs, scientific and research projects, and warfighting capabilities.

The DIB CS/IA pilot is informing proposed changes to the DFARS for enhanced IA/CS requirements in DoD contracts.

To continue improvements in DIB network security, the Department of Homeland Security, in collaboration with the Department of Defense, is evaluating the DIB model for sharing cybersecurity information with other Critical Infrastructure sectors.

International Program

The Department has a very robust program built on trusted bilateral, multilateral, and institutional relationships with national and military representatives around the world to enhance situational awareness and capabilities to counter common cyber threats, share tactics, techniques and procedures and synchronize IA/CS strategies and policies. Shared situational awareness helps stay ahead of the threat, protects U.S. secrets and sensitive information residing on foreign networks, and protects coalition and allied operations, especially with increased ops tempo for counterterrorism activity and for peacekeeping. Cyber attacks in Estonia and Georgia have accelerated international cooperation. A common objective is to promote adoption of international standards and norms in partnership with interagency processes. This includes developing common positions for international fora, influencing standards and technology, and discussing international norms of behavior in cyberspace.

We have a number of bilateral agreements with partner countries and are aggressively pursuing more. Current activities include the International Computer Network Defense

(CND) Coordination Working Group (ICCWG), the International Cyber Defense Workshop (next one is June 2009), international civil and military participation in Cyber Storm II, (a large-scale national cyber exercise part of Homeland Security's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector), and the ongoing sharing of best practices, policies, and threat information. Challenges in this area include limited classified network connectivity, over-classification of information, and difficulties in applying "write for release" practices for cybersecurity information sharing.

Goal 2

Next I will highlight two initiatives under Goal 2 (Enable mission driven access to information and services). They are identity management and assured information sharing.

Identity Management

Our identity management (IdM) initiative provides the ability to identify people and devices on our networks and distinguish among friendly, neutral, and unfriendly entities. Our Identity management capabilities are based on use of public key infrastructure (PKI) technology. Our public key certificates and the Common Access Card (CAC) provide strong, highly trusted electronic identity credentials for our people and our non-person entities (e.g., network and computer devices, phones, radios, satellites, services, applications, etc.). The Department's PKI and IdM efforts are base-lined on the Homeland Security Presidential Directive 12/Personal Identity Verification (HSPD-12/PIV) standard for the Federal Identity Credential. Nearly all of the Department's Active and Reserve military, civilian employees and contractors utilize CACs to facilitate network, web site, and facility access. Adherence to the HSPD-12/PIV identity credential standard makes it possible for federal partners to use their PIV cards to access DoD information repositories and web servers with enhanced user security.

The Department's use of hardware-based identity credentials for access to networks and information systems has shut down known attack vectors, demonstrably decreased attacks, and elevated the security posture to our networks by denying anonymity to attackers. The use of biometrics in conjunction with PKI credentials is yielding important improvements in protection against insider threats. Identity interoperability with industry and international groups will help with secure information sharing and force protection.

DoD is involved in two premier programs leveraging standardized identity credentialing. They are the Transglobal Secure Collaboration Program (TSCP) and the Federation for Identity and Cross-Credentialing Systems. The DoD and industry have partnered through the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) to verify the identity of personnel and accept each other's identity credentials. FiXs currently verifies and authenticates the identities of contractor personnel seeking to enter U.S. military installations or other government controlled areas.

The Transglobal Secure Collaboration Program (TSCP) is a government-industry partnership specifically focused on facilitating solutions to the most critical issues in Aerospace and Defense (A&D) today: A key enabler for the TSCP is a common identity approach that is highly aligned with the HSPD-12/PIV credentialing program. Their interoperable identity credentials mitigate the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions. To do business in the world today, A&D companies must balance the need to protect intellectual property (IP) while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information. This duality requires that security be both within organizations and across extended supply chains and partners.

Assured Information Sharing

In addition to sharing information among trusted users across organizational boundaries, the Department is working hard to enable sharing across the entire spectrum of security domains while protecting networks and information. To that end, it partnered with the DNI and established the Unified Cross Domain Management Office (UCDMO) in 2006. The UCDMO is staffed with personnel from throughout the Department of Defense and the Intelligence Community (IC); it provides centralized coordination and oversight of all cross domain activities and ensures a common approach for the implementation of cross domain capabilities within the Department and the IC. Additionally, it is working to ensure that secure, robust and flexible capabilities are available and extensible to share information among federal, state, local and tribal entities and with mission partners and private sector enclaves appropriately. The UCDMO roadmap is aligned to the information sharing strategic plans of the Department and the IC, and it is focused on delivering needed sharing capabilities, providing return on investment, managing security risk, and promoting awareness and collaboration among the users and developers.

Goal 3

From Goal 3 (Anticipate and prevent successful attacks on data and networks) I will highlight two initiatives; network de-militarized zones and host-based security. This goal is focused on hardening data and networks in order to anticipate and prevent successful attacks on them. The most capable and motivated of our adversaries will use any means available to achieve their goals, and our strategy must address that range of tactics. To that end, we invest in intelligence and perimetèr-hardening to anticipate and prevent successful attacks, but we also design and configure systems to ensure that attackers are easy to find and/or contain should they pierce perimeter defenses.

De-militarized zones

Network de-militarized zones (DMZs), are to perimeter defense as a moat is to a castle. The DMZs obviate the need for most DoD assets to ever have to touch the Internet. Instead, those DoD applications, such as email, which must face the Internet are housed within a special containment zone. Within that zone inward-bound traffic can be carefully scrutinized for viruses and other malware. The DMZ controls can also enforce white-listing, that is, only allowing traffic from trusted addresses to enter the enterprise, and perhaps most importantly, by acting as a proxy for all communication to the untrusted world, can deny adversaries reconnaissance knowledge of the structure of DoD networks. The Department has vastly reduced the number of its Internet access points, the first step in moving toward an enterprise-wide DMZ architecture, and is identifying outward-facing applications for placement in the zones.

While DMZs harden the network at entry points, host-based security provides a line of defense at each computer. Host-based security significantly reduces the risk of cyber attack at the individual computer by preventing malicious code and unauthorized applications from running. It also provides a consistent way to do configuration and management across all DoD networks.

Host-based security

Host-based security includes, but is not limited to host firewall, host intrusion detection, host intrusion prevention, system compliance profiling, rogue system detection, application blocking, and Information Condition (INFOCON) baselining. Under USSTRATCOM's direction, the Department is rapidly implementing host-based security across the enterprise. It is now deployed within approximately 40% of the host processing environment, and should be deployed to a majority of our systems by early 2010. Coupled with this, we are widely deploying the Federal Desktop Core

Configuration, a pivotal industry/government cooperative venture, beginning with ubiquitous Microsoft products, to make computers more stable and defensible. We are also widely deploying data-at-rest protection.

As is evident from these highlighted projects, safeguarding our networks against adversary attack today requires close partnership between information assurance experts and information technology (IT) providers. The DMZs are as much about network architecture as they are about specific tools for content filtering, and host-based security is a suite of software which is installed on commodity computing hardware; it is not a stand-alone IA device that plugs in to a computer or network. This convergence of IA/CS and IT poses challenges for governance and training, but it promises some new and much more efficient ways to secure our networks.

Our DoD research labs are particularly interested in new IT paradigms that change the game for defense, and I will close this section by discussing two of them, virtualization and cloud computing, which together and separately may revolutionize how we think about and secure our networks.

Virtualization

The DoD enclaves today look mostly like traditional local area networks; each user has a physical device on a desk linked back to one or more servers. Some user data lives on the desktop machine and some resides on servers, with the desktop patched periodically to close security holes and implement new configuration guidance. With virtualization, the necessity for coupling together specific logical and physical assets goes away. For example, each user's environment (data and computing tools) can be stored and maintained as a digital file or image in a central control area. When a user needs their environment, it can be "incarnated" into any compatible physical platform. So tomorrow, instead of scanning physical components for current state and applying patches to bring the component into compliance, we may, instead, proactively repair and refresh the stored images and only incarnate the good ones. Doing this cleverly and often will make it harder for adversaries to sustain the footholds they gain through phishing attacks to persist in our networks.

Cloud computing

Cloud computing builds on these ideas to offer a virtual computing fabric with almost limitless and infinitely definable processing and storage capacity. In the future, many enterprises will choose not to invest in their own IT departments, but will pay as they go, relying on ability to access commercial computing services in the cloud. For many DoD applications, the commercial cloud will be too risky, but a private cloud could bring us many benefits. Besides the obvious economic benefits of scalable, on-demand computing, a private cloud also gives us the ideal platform with which to provide the virtual monitoring and provisioning described earlier. A cloud is also an ideal place from which to make capabilities available to the whole enterprise. While, in the DoD, we have encountered challenges moving towards a service-oriented architecture (SOA), in the private sector, companies like Google and Salesforce are basing their business models on an insatiable public hunger for software and applications as a service. Emulating their delivery mechanisms within our own private cloud may be key to how we realize the true potential of net-centricity.

Goal 4

Finally, I will highlight three initiatives under Goal 4 (Preparing for and operating through cyber attack or degradation) which provides a foundation to leap beyond traditional IA/CS approaches. They are supply chain risk management, assurance in defense system acquisitions, and network resiliency.

Supply Chain Risk Management

While the global marketplace provides the Department increased opportunity for innovation in information and communication technologies (ICT), it also provides increased opportunity for malicious actors to manipulate ICT products and services to gain unauthorized access to otherwise closed-off technologies and services – what we call supply chain risk.

Threats to the ICT supply chain can affect both software and hardware products. Software design, development, testing, distribution, and maintenance frequently can be done less expensively offshore, but puts technology within easy reach of malicious actors. At the same time, the growing complexity of software and microelectronics makes discovering vulnerabilities extremely difficult. Security of the ICT supply chain can also be compromised by untrustworthy or counterfeit ICT components. We are particularly concerned about the semiconductor industry which has increasingly moved toward offshore or foreign-owned semiconductor component production. This trend creates an increasing threat to the US as the potential for unauthorized design inclusions to appear on integrated circuits used in military applications increases.

As early as 2003, the Department promulgated a Defense Trusted Integrated Circuits Strategy. The Trusted Foundry Program, initiated in fiscal year 2004, leverages a contract with IBM to aggregate purchases of leading edge semiconductors with state-of-the-art features for use in defense applications. As part of the contract, IBM upgraded their facilities and implemented enhanced security procedures, creating the Department's first Accredited Trusted Integrated Circuits Supplier. In 2004, the Department tasked the NSA to stand up a new office to manage this contract and expand the ranks of suppliers capable of providing trusted integrated circuits. In response, NSA created the Trusted Access Program Office and implemented a trusted integrated circuits supplier accreditation program, now overseen by the Defense Microelectronics Agency.

The Trusted Foundry Program is funded at approximately $80M/year through equal investments from the Services and NSA as well as from direct program payments for chip processing and services. In 2008, the Trusted Foundry served over 80 program customers and processed 412 unique integrated circuits designs. The Trusted Supplier

Accreditation program continues to expand and there are now 21 Accredited Trusted Suppliers providing a full range of services enabling the department to draw on a fully accredited end-to-end trusted supply chain for integrated circuits.

Building on the Trusted Integrated Circuits Strategy, the Department continued to work supply chain risk issues both internally through DoD software and systems assurance efforts beginning in 2004, and within the interagency through the Committee on National Security Systems. Its strategy is holistic: System prioritization allows the Department to apply resources first against our most critical systems; an approach to driving assurance activities into the systems engineering process, to identify critical sub-systems and components, and to mitigate vulnerability through engineering design; a supplier assurance process to increase knowledge of counterintelligence threats posed by the suppliers' chain; a technology strategy to improve vulnerability detection capability, and a collaborative effort between DoD and industry to identify standards and best practices. This approach was validated by a September 2007 Defense Science Board study "Mission Impact of Foreign Influence on DoD Software," and informed subsequent efforts within DoD and the interagency.

The Department now co-leads an interagency effort with the Department of Homeland Security to develop a multi-pronged, US Government (USG)-wide approach to global supply chain risk management for hardware and software ICT. This effort brings to bear a range of USG capabilities to address national security risk to USG systems and networks from globally developed and maintained ICT through sharing of technical risk mitigation techniques, development of new acquisition guidance, work with industry on the promulgation of commercial standards, and enhancement of IT and software assurance capabilities. The Department has recently issued policy for managing supply chain risk to ICT within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23. Additionally, the policy establishes Department-wide responsibilities for meeting the assessment and reporting requirements of §254 of the Fiscal Year 2009 National Defense Authorization Act.

The Department is incrementally developing a supply chain risk management (SCRM) capability, beginning with pilot activities in fiscal years 2009-2010 and progressing to full operational capability by fiscal year 2016. These pilots are a joint effort led by the Deputy Assistant Secretary of Defense for CIIA. Each of the military services and DISA has identified pilot programs to test SCRM engineering and procurement processes and mitigations and share best practices. The Department is also partnering with the IC in evaluating the risk to the Department posed by commercial entities conducting business with the individual components of the Department.

Ultimately the goal of the SCRM pilots is to position supply chain risk management decision-making very early in the system lifecycle. Early identification of risk facilitates mitigation through system design and ensures that ICT products purchased for use on DoD systems and networks are sufficiently trustworthy for their intended purpose.

Assurance in Defense System Acquisitions

Complementary to the SCRM efforts are the DoD CIO's responsibilities for overseeing the integration of IA/CS into major defense system acquisition programs to ensure compliance with statute, and consistency with DoD policies, standards and architectures. Under Subtitle III of Title 40, United States Code (formerly the Clinger-Cohen Act of 1996), the Department conducts formal reviews of the acquisition IA strategies of all Major Automated Information Systems (MAIS) and Major Defense Acquisition Programs (MDAP) prior to approval of all acquisition milestone decisions. The acquisition IA strategy sets the stage for early, effective, and efficient implementation of IA into the system.

The Department emphasizes the early identification of IA/CS requirements for all IT acquisitions, including weapons systems and command and control systems. An IA/CS controls-based approach is employed that mandates a comprehensive set of protection requirements based on the sensitivity of the information and the importance of the mission that the system supports. The specific IA/CS technical solutions that satisfy the individual IA/CS controls must be certified as effective and secure before implementation into the systems. Leading-edge networking programs are required to comply with similarly leading-edge information security requirements from NSA to ensure that new capabilities are protected. Finally, the system as a whole is subjected to a rigorous independent security review and an overall risk management decision prior to allowing it to operate. The Department is working to streamline the fielding of ICT commercial solutions, accelerate the certification and accreditation process, and achieve greater reciprocity of IA/CS risk management processes and decisions across the Department and federal government.

A particular challenge in this area is acquisition time. Our reliance on globally sourced ICT means our adversaries have access to the same technologies we do; however, our ICT and IA/CS acquisitions must follow the same rules as for weapons systems, constraining our ability to respond quickly. We need more agile ICT and IA/CS acquisition processes. Acquiring automated information systems without a production component is significantly different from acquiring a weapons system. For weapons systems we concentrate on key risk areas like technology maturity and producing large numbers of custom hardware in economic quantities. In contrast, for automated information systems we concentrate on reducing risk in areas like process reengineering, enterprise architectures, information assurance, and integration of multiple commercial off-the-shelf applications.

The challenges of information technology acquisition were studied by the Defense Science Board as directed in the fiscal year 2008 National Defense Authorization Act. The results of their study were recently released (April

2009) and recommended changes to our acquisition processes, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. A process that is agile and geared to delivering meaningful increments of capability in approximately 18 months or less.

DoD has recently instituted a new rapid intergovernmental acquisition process that develops multiple competitively-awarded Blanket Purchase Agreements (BPAs). In partnership with the General Services Administration (GSA), this process provides BPAs in six months for heavily discounted IA/CND products available for federal, state, local, and tribal government agencies.

Network Resiliency

Denial of service against critical elements of the physical and application layer of the networks and cyber attacks effecting the integrity and confidence of information flowing to users and decision makers is increasingly a major source of risk, as shown by recent undersea communications cable cuts or threats by software worms like Conficker. The Department's Guidance of the Development of the Force (GDF) for 2010-2015, signed May 2008 states, "All DoD Components will reduce the risk of degraded or failed missions by developing doctrine/tactics, techniques and procedures and planning for, implementing, and regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid."

In support, we have a series of cyber resiliency and mission assurance initiatives that are focused on reducing risks to missions should our networks, enterprise services, or information be compromised or degraded. They include:

- Exercising military operations under a severely degraded cyber environment.
- Improving prioritization for recovery and continuity of operations planning.
- Strengthening network command and control capabilities.

While the Department is aggressively enhancing the security of the GIG and promoting IA/CS nationally and internationally, the threats in an information-centric world are dramatic. Conducting counterterrorism operations, global peacekeeping, homeland security and preparing for escalated warfare make it imperative that IA/CS be viewed not as an IT expense but as a critical enabler of all national security and defense capabilities. To this end, the Department sees its participation in the Comprehensive National Cyber Initiative (CNCI) as imperative. The Department leads or co-leads several CNCI initiatives:

- Initiative 3, with the NSA supporting Department of Homeland Security efforts to secure the .gov domain.
- Initiative 7, with the Department and the DNI co-leading an effort to secure the classified networks.
- Initiative 8, with the Departments of Defense and Homeland Security developing the conceptual foundation for building the USG cyber workforce of the future and reinforcing the skills of the current workforce.
- Initiative 11, previously discussed under SCRM.

Summary

In conclusion, the Department has a strong IA/CS vision, strategy and supporting program. We are working toward a resilient and defendable core network for the Department and for the nation. The ASD(NII)/DoD CIO is managing a diverse portfolio to lead the Department toward Net Centric operations and aggressively working to get ahead of the daunting security challenges facing the Department.

Ms. WATSON. You may proceed.

STATEMENT OF JOHN STREUFERT

Mr. STREUFERT. Good afternoon, Madam Chairwoman Watson, Ranking Member Bilbray, and distinguished members of the subcommittee. I am pleased to have this opportunity to testify before the subcommittee regarding the Department's of State capabilities for combating cyber threats, detecting and mitigating vulnerabilities, and securing the Department's global information and technology infrastructure. My statement will describe key elements of the Department's information security program.

Madam Chairwoman, as you know from your time at the Department of State, we serve as the diplomatic front line in over 270 overseas posts. This global reach affords the Department a unique perspective on cybersecurity as we provide for the confidentiality, integrity, and availability of a worldwide network for the 50,000 users of the Department and the application software that they put to work. The foreign policy mission makes an inviting target for attack by highly skilled cyber adversaries.

However, the Department's layered approach to risk management allows multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls. In my dual roles as Chief Information Security Officer and Deputy Chief Information Officer for Information Security, I am part of an integrated team. Together, technical and operational security experts of the Department work in close coordination with the DOD and others to satisfy mission essential requirements from our command and control capabilities, network and critical infrastructure protection, law enforcement, and intelligence community support.

The scope of cyber activity the Department faces in a typical week includes blocking 3½ million spam emails, intercepting 4,500 viruses, and detecting over a million external probes to our networks. The Department maintains a 24 x 7 network watch program that guards against external penetration, compromise, or misuse of the Department's cyber assets.

Analysts stationed at our network monitoring center serve as continuous sentries for inappropriate network activity. The analysts perform preliminary assessments to confirm the nature and source of suspicious network security events. Those matters deemed significant are escalated to our Computer Incident Response Team [CIRT], for in depth analyses and corrective action. CIRT analysts track all reported actions through completion and coordinate incident response actions with all stakeholders including our internal Department security units, the Department of Homeland Security, US-CERT, and law enforcement entities.

To combat increasingly sophisticated cyberattacks, the Department's of State Cyber Threat Analysis Program provides early warnings about potential cyber incidents. This team of technical analysts performs essential in depth assessments of network intrusions and helps to coordinate the Department's response to sophisticated cyberattacks. In addition, they perform proactive penetration testing and network forensic analyses to detect and resolve significant threat issues.

The Global Security Scanning program at the Department serves multiple essential purposes covering all of its domestic and overseas locations. Electronic tools perform functions that include confirming what is connected to the Department's networks; assuring that computers, networks, and software are in the safest of configuration settings; locating system vulnerabilities that need correction; and collecting evidence for cybersecurity investigations. Global Scanning is complemented by our computer security officers that are posted both regionally and locally for overseas embassies and consulates as our boots on the ground.

To strengthen its operational capability, the Department has created the Risk Scoring Program to help pinpoint and correct the worst network and system vulnerabilities on any particular day both locally and for our networks worldwide. Risk points are assigned for cyber threats consistent with vulnerabilities defined in the National Institute of Standards and Technology guidelines.

Every computer and server connected to the Department of State network is scanned worldwide on a continual basis. Based on progress in reducing vulnerabilities overseas and at headquarters organizations, each entity is graded from an A to an F for their work during the last month. In this sense, it functions like a daily quiz where at the end of the month there is a test and a grade is given.

Madam Chairman, we are pleased to report that an embassy as far flung as the one in Kolonia where you served currently has an A+ with perfect ratings in 6 of 10 categories we evaluate, notwithstanding how far it is from many other industrialized centers.

Since July 2008, overall risk on the Department's key unclassified network has been reduced by nearly 80 percent in overseas sites and 55 percent in domestic locations.

The Department's Cybersecurity Incident Program was formed to address consequences for acts of cyber misuse or abuse by individuals. The Cybersecurity Incident Program applies to all Department system users and defines infractions and violations. More serious violations are cases where the failure to comply with a specific Department policy exists and results in damage or the potential of significant damage to the Department's cyber infrastructure. Along the notification of an incident, an investigation is undertaken incorporating several Department organizations charged with gathering what is necessary to ensure a prompt and appropriate response to the cyber event while protecting the rights of the accused.

For those that are found to have committed an infraction or violation, the consequences available to the Department range from a letter of warning to suspension of network access. In select cases, further disciplinary action has been recommended or referral for criminal prosecution.

Madam Chairwoman, I want to conclude by reiterating that the Department's strategy and programs are continually adapting to match the ever changing threats to cybersecurity. We believe we have the policies, technology, business processes, and partnerships in place to evolve and meet the continuing challenges of security threats in the cyberspace environment.

I thank you and the subcommittee members for this opportunity to speak before you today. I would be pleased to respond to your questions.

[The prepared statement of Mr. Streufert follows:]

Statement of
John Streufert

Chief Information Security Officer /
Deputy Chief Information Officer for Information Security
Bureau of Information Resource Management
United States Department of State

Cybersecurity: Emerging Threats, Vulnerabilities and Challenges

House Subcommittee on Government Management,
Organization and Procurement,
Committee on Oversight and Government Reform

2154 Rayburn House Office Building
May 5, 2009
2:00 p.m.

Good afternoon Madam Chairwoman Watson, Ranking Member Bilbray, and distinguished Members of the Subcommittee:

I am pleased to have this opportunity to testify before the Subcommittee regarding the Department of State's capabilities for combating cyber threats, detecting and mitigating vulnerabilities, and securing the Department's global information and technology infrastructure. My statement will describe key elements of the Department's information security program.

Madam Chairwoman, as you know from your time at the Department of State, we serve as the "diplomatic front-line" in over 270 overseas posts. This global reach affords the Department a unique perspective on cyber security as we provide for the confidentiality, integrity and availability of a worldwide network, 50,000 users and the systems they use. The foreign policy mission makes an inviting target for attack by highly skilled cyber adversaries. However, the Department's layered approach to risk management allows multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect and mitigate vulnerabilities, and strengthen business operations.

In my dual role as the Chief Information Security Officer and Deputy Chief Information Officer for Information Security, I am part of an integrated team. Together technical and operational security experts of the Department work in close coordination to satisfy mission essential requirements ranging from command & control capabilities, network & critical infrastructure protection, law enforcement and intelligence community support. The scope of cyber activity that the Department faces, in a typical week includes blocking 3.5 million spam e-mails, intercepting 4,500 viruses, and detecting over a million external probes to our network.

Network Monitoring & Incident Response

The Department maintains a 24/7 network watch program that guards against the external penetration, compromise, or misuse of the Department's cyber assets. Analysts stationed at our Network Monitoring Center serve as continuous sentries for inappropriate network activity based on intrusion detection system signatures, reports from the Firewall Team and other sources. The analysts perform preliminary assessments to confirm the nature and source of suspicious network security events. Those matters deemed significant are escalated to the Computer Incident Response Team (CIRT) for in-depth analysis and corrective action.

The CIRT serves as the Department's main clearinghouse for reporting computer security events and incidents occurring on Department and foreign affairs agency networks. CIRT analysts track all reported actions through completion and coordinate incident response actions with all stakeholders including the Department's security units, Department of Homeland Security's US-CERT and law enforcement entities.

Threat Detection

To combat increasingly sophisticated cyber attacks, the Department's Cyber Threat Analysis Program provides overseas posts and Department management with indicators and early warnings about potential cyber incidents. This team of technical analysts perform essential in-depth assessments of network intrusions and help coordinate the Department's response to sophisticated cyber attacks. They also work closely with the law enforcement and network defense communities to develop both a comprehensive threat picture and possible remediation measures. In addition, they perform proactive penetration testing and network forensic analysis to detect and resolve significant threat issues.

Global Security Scanning

The Global Security Scanning program of the Department serves multiple essential purposes covering all of its domestic and overseas locations. Electronic tools perform functions that include confirming what is connected to Department networks; assuring that computers, network and software are in the safest configuration of setting, locating system vulnerabilities that need correction and collecting evidence for cyber security investigations. Global scanning is complimented with computer security officers supporting security regionally and locally for overseas posts as "boots on the ground."

Vulnerability Management

To strengthen its operational capability, the Department created the Risk Scoring Program to help pinpoint and correct the worst network and system vulnerabilities on any particular day and networks world-wide.

Risk points are assigned for cyber threats consistent with vulnerabilities defined in National Institute of Standards and Technology (NIST) guidelines. Every computer and server connected to the State Department network is scanned world-wide on a continual basis. When the risk scoring program began approximately two thirds of the calculated risks including vulnerabilities were found at domestic locations. Total risk points are calculated for each organization each day, and when vulnerabilities are corrected the total risk points are reduced. Based on

progress in reducing vulnerabilities each overseas and headquarters organization is graded from "A" to an "F" for their work during the last month.
Since July 2008, overall risk on the Department's key unclassified network, measured by the Risk Scoring pilot components, has been reduced by nearly 80% in overseas sites and 55% in domestic sites.

Consequences for Cyber Misuse or Abuse

The Department's Cyber Security Incident Program was formed to address consequences for acts of cyber misuse or abuse by individuals. The program enhances the protection of the Department's cyber infrastructure by raising overall cyber security awareness and providing managers with the ability to hold individual users accountable for acts of cyber misuse or abuse. The Department like all parts of the federal government needs to balance the benefits of cyber space for mission effectiveness, with the personal responsibility every employee is asked to demonstrate when using government cyber resources.

The Cyber Security Incident Program applies to all Department system users and defines two different categories of incidents: "infractions", where failure to comply with a specific Department policy exists but does not result in actual damage to the Department's cyber infrastructure and "violations", where failure to comply with a specific Department policy exists and results in damage or significant risk of damage to the Department's cyber infrastructure.

In addition to the types of incidents that lend themselves to detection, the Department's network monitoring and inspections alert key Department officials to risks when they occur. Upon notification of an incident, an investigation is undertaken incorporating several Department organizations charged with gathering the information necessary to ensure a prompt and appropriate response to the cyber event, while protecting the rights of the accused.

Since the Cyber Security Incident Program was established in 2007 a total of 82 users have been cited for infractions and 14 users have been cited for violations. For those found to have committed an infraction or violation, the consequences available to the Department range from a letter of warning to suspension of network access. Select cases resulted in further disciplinary action or referral for criminal prosecution.

Other Federal Activity

The Department of State is involved in multiple government-wide efforts that share its IT security solutions with other Departments and Agencies. The most widely use product is an annual IT security awareness course offered to other federal organizations as a Center of Excellence under the Information System Security Line of Business. So far this offering has been delivered to 33,255 federal employees from outside the State Department. The State Department is also active in multiple projects with the inter-agency Committee on National Security Systems working on developing common standards for risk studies and authentication of users on networks.

Madam Chairwoman, I want to conclude by reiterating the Department's strategy and programs are continually adapting to match the ever changing threats to cyber security. We believe we have the policies, technology, business processes, and partnerships in place to evolve and meet the continuing challenges of the security threats in the cyberspace environment. I thank you and the Subcommittee members for this opportunity to speak before you today and would be pleased to respond to any of your questions.

Ms. WATSON. Thank you so much for your testimony. We are now going to move to the question period and proceed under the 5-minute rule. I will make my statement and than I will recognize the ranking member, Mr. Bilbray for 5 minutes as well.

These questions will be for both panelists. You can respond as soon as I finish. When we talk about cyberattacks against Government agencies, we often fail to determine the purpose of the attacks being carried out such as those for economic gain, espionage purposes, or simply to disable or to disrupt Government operations. If possible, I would like both of you to offer some general observations on the differences or the similarities between cyberattacks from both domestic and international sources. Are there distinguishable motives or things for either source? Do certain groups target specific networks or cyber infrastructure in their activities, or do they look for the weakest link in the chain for attack?

I am very pleased that Kolonia in the Micronesian Islands is following a good example and that they are A+. That is a little personal thing, there.

But if you will start, Mr. Lentz, I would appreciate it.

Mr. LENTZ. I think your question is a very good one because the state of cyber threats has changed dramatically over the last several years. In fact, what we are seeing in the past 18 months is a significant rise in cyber crime activity, a significant rise. Before that, it was pretty much exclusively in the hacker domain where we would get a lot of our cyber events occurring. That skill set has dramatically improved in terms of its skill craft as well.

But going to your question, the state of play, because cyber criminals now can use the Internet to make lots of money, provides them a playing field that is very rich with targets of opportunity. So that is a significant concern of all of us, particularly other sectors of the U.S. Government and of course the private sector.

But the other aspect of this is one that we in the Department of Defense are of course always concerned about, the threat against our national security systems and our weapons programs. We always have to be prepared for a nation-state or surrogate of a nation-state to take action against our networks either for espionage or for other denial of service purposes in conflict. So that is the other aspect of this problem, which is continuing to grow in sophistication. It is one that we are very concerned about and we have to be prepared for.

Ms. WATSON. Mr. Lentz, naturally there is probably little you can tell us in an opening statement or in your statement about the recent breeches to the Joint Strike Fighter and Marine One programs. But I do, however, feel obligated to ask you about some general background that is consistent with what is part of the public record. So can you tell us where you are in determining the sources of the breeches and whether they were government sponsored or private cyber criminals at work there?

Mr. LENTZ. As you said, Madam Chairwoman, this issue is very sensitive. We are prepared to give the committee a classified briefing of the details of the investigation. Much of this investigation right now is held in law enforcement channels under warrants. It is an ongoing investigation. That is the current position where we are. It is a very important priority of ours to get to the bottom of this.

Ms. WATSON. I know that technology improves every single day. I am wondering if the personnel who work on our posts are well equipped with the knowledge of how it operates and the uses. Do you then train, say the new Ambassadors and the embassy staffs, along these lines of the increases in technology?

Mr. LENTZ. Training and education awareness is without a doubt one of our top priorities. In my opinion, I think it is our most important priority because people are what run our network. We improve awareness training every single year. One of the things that we are doing a lot more of, to go to the heart of your excellent question, is leadership training. That is one of our highest priorities right now, to the highest levels of our Department, to make sure that general officers and senior officials coming into the Department are briefed in an in depth form on the cyber threat. It is a very big priority to include our mission partners in places like embassies to make sure. We team with State Department in collaborative efforts to do the same thing.

Ms. WATSON. Mr. Streufert, do you want to comment?

Mr. STREUFERT. To your question of training, we place an extraordinarily high value on the current Federal Information Security Management Act. It encourages that there is annual awareness training. At the State Department, by one method or another, we provide sometimes oral briefings to the most senior leadership of the Department of State, or in other cases, remote distance learning. For the balance of the Department, we see training to be extraordinarily beneficial as our users are an important part in the protection of the information that the Department of State has and what we are asked to protect.

The State Department has initiated a pilot project for a method of training called Tips of the Day. What we do, when the computer users log on in the morning, is to provide them two or three sentences of instruction and then, to those connected in what we expect to pilot in two of our bureaus here in the coming weeks, a true/false question. Then we keep track of those answers and the level of understanding about basic security awareness.

We found this to be a particularly beneficial mechanism at an earlier point of testing after a laptop was lost in one part of the Government. This occurred at USAID. We very quickly went out and reinforced that personally identifying information should not be carried out of a Government space without prior arrangements, which has evolved to become encryption to later events.

So along with Mr. Lentz, we believe that training is a very essential part to keep our users leaning forward to complement the important changes we make in technology.

Ms. WATSON. My own time is up. I will recognize the ranking member, Mr. Bilbray, for 5 minutes.

Mr. BILBRAY. Thank you, Madam Chair. Thank you for having a loud mic this time around. I appreciate the technology advancement.

Mr. Lentz, sadly there are a whole lot of things we can’t talk about here in public. So I guess that is sort of an indication of how important this issue is going to be.

There is a lot of discussion about how secure our systems are within the structure and whatever. But I want to sort of back off and go down to the fact of who has access into these systems, especially the contractors. Right now, within the Department itself, we verify before we hire somebody in house who they are and what they are. We use E-Verify to classify that, right? Within the Department itself, we use E-Verify?

Mr. LENTZ. That is right.

Mr. BILBRAY. But we have delayed—correct me if I am wrong, you may be doing this with your contractors—but right now the administration has delayed the implementation of E-Verify from February I guess until late June. Are you now with your contractors that are being brought in to work on a lot of these projects, are you now by policy requiring e-verification of every employee so we know they are who they are, or at least have the justification to know that the Social Security and other information they have given is viable?

Mr. LENTZ. My understanding is we do not use E-Verify within the Department of Defense. So I can't really respond to that particular question. We can take that for the record and talk to DSS and get some specifics.

Mr. BILBRAY. I just think that kind of the minimum is that we make sure that everybody is checked. As far as I know, you are supposed to be using it in house. Members of Congress use it. Everybody in the Federal system is supposed to be E-Verifying whenever we hire.

The trouble is when we bring the contractors in. We have had situations where contractors have been working on nuclear powered ships and it was a major concern. I just want to make sure that we put the same level of security on our information systems that we put to our nuclear ships. That is make sure that any contractor who is coming in, who has access to our systems, has at least been checked that they are who they claim to be. That is the first level of security we ought to talk about.

So I would ask that you take a look at that. I think, God forbid, we wouldn't want to have next month come out and everyone say, well, why didn't we implement this earlier. There were things that Congress couldn't even discuss in public but people that hadn't been checked were being allowed into the system. I ask that we see what kinds of systems, first of all, we have to make sure the access into the system is only people that have been qualified.

In that category, generally what efforts underway do we have to secure the contractors' networks and their material?

Mr. LENTZ. First to go back to your first question, one program that we have instituted in the Department of Defense is a program called FICS, which stands for Federated Identity Credentialing Service. It is a program we have working with industry to, in a federated way, to recognize their security clearance process. Then using electronic authentication capabilities, we can in fact recognize their entrance into the Department of Defense installations.

Mr. BILBRAY. Now that electronic, is that biometric or is that just the pass card system?

Mr. LENTZ. It is currently using PKI, Public Key Infrastructure technology. That is the same technology we use in the Department of Defense to implement Homeland Security Presidential Directive No. 12 pervasively throughout the Department. So that technology is proven.

Mr. BILBRAY. Is there biometric confirmation in that?

Mr. LENTZ. It does not currently leverage biometrics but we do have a program for three factor authentication underway to pilot that throughout the Department.

To the other part of your question, we have our defense industrial base effort that we launched a little less than 2 years ago. That effort is aggressively going after the control of unclassified information that resides on our contractor systems. We have a pilot underway with a number of our top industrial partners to help protect their networks to the same level that we are protecting our own.

As I mentioned in my oral remarks, this program has proven to be very successful both in getting very timely threat information to our industrial base partners, but also for them to provide us very timely information on incidents that they have occurring on their networks. We use a very strong policy framework and legal framework to protect the equities of each of us to make sure that information flows near real time if at all possible.

Mr. BILBRAY. Madam Chair, I wasn't planning on following this line but I have sort of fallen into the fact that the first line of defense against somebody messing with our information system is to make sure the people we hire to help do the work aren't people we don't want on there.

I have just quickly a question because my time is up. Do we have the same access system going into the Pentagon today that we had during 9/11? It sure looked like the same system to me. Have we upgraded and put biometrics or anything else on the Pentagon?

Mr. LENTZ. No, sir.

Mr. BILBRAY. I just think that is something we need to talk about in the future. I appreciate it, Madam Chair.

Ms. WATSON. Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chair. Let me ask each of you, in your respective agencies, what keeps you up at night? What is your sense of the biggest threat you worry about? Is it hacking into the system? Is it just a breech of security because somebody is not careful? Is it unwarranted inquiries into classified and/or unclassified systems? Is it the far flung enterprise you each represent?

Mr. Streufert, I think you mentioned 280 locations around the world for the State Department. There must be an equal number in the Defense Department. Levels of security have to very given that far flung enterprise.

I would just like to have some sense from each of you in terms of the Defense Department and the State Department of your sense of the nature of the threat and how well equipped we are from your point of view to address that threat.

Mr. STREUFERT. Congressman, an aspect that keeps me up at night is precisely the one that you mention on how far flung the Department of State is, particularly in conjunction with the comments that a number of Members have made and Mr. Lentz about how sophisticated and evolving the threat is.

The reality is that we could have new threats which would appear overnight. In practical terms, if we don't have a tool that is capable of diagnosing that threat, we could have difficulties that could get away from us and potentially cause harm.

So I think that the future of protecting Federal networks is likely to aim in the direction of trying to find those sets of tools that could be made available to those within the .gov network, which you made appropriate reference to, to figure out how we can protect the information that the American public entrusts with those of us at the national level and distributed throughout the other parts of the Federal Government and in the States. I think that is a very challenging area. We just have to watch the continually evolving threats and figure out a way that we can step up to them.

Mr. LENTZ. As Chairwoman Watson said, what keeps me up at night is the pervasiveness of this threat when we talk about cyber espionage and the amount of information that is getting stolen, from not just the Government's potential networks but the Nation at large. The technology edge that we have currently, especially when it comes to innovation, is one that we have to protect very, very carefully. I think that keeps me up at night, not only as a Government employee but as a private citizen.

The second thing is, from a DOD standpoint, the threat of a nation-state in terms of what it can do if hostilities rise to that point. We have to have the best protection mechanisms in place and redundancy in our capability to withstand a very sophisticated nation-state, in light of the fact that all of our systems and networks and people are now so dependent upon the network and information to be successful, as we see in the Information Age. Those are the two things that keep me up.

Mr. CONNOLLY. The suggestion has been made that the very nature of the architecture of the Internet as such an open system, so all-encompassing, that by its very nature it is subject to compromise. There is just no getting around it. Have you given thought to creating parallel systems that are closed for the U.S. Government? Would it work?

Presumably, the same techniques for hacking into or compromising even a secure system on the existing Internet could likewise be applied to a parallel closed system. I would be interested in whether your respective agencies have examined that and what you think about the practicality of it.

Mr. STREUFERT. This is an area that we looked to under the Committee on National Security Systems, in which Mr. Lentz plays a very active part and I am privileged to participate at a number of their activities each year. There are some technologies that are being worked on in the Department of Defense that seem to hold the best prospects for protecting information of national security importance, but also of the nature of protecting personally identifying information as an example.

The use of the Internet has both risks and potential benefits for the American public. As an example, with the consular function, which I know the Madam Chairwoman understands very well, we are able to support the needs of the public through some online activities which make it easier for people at a distance to obtain visas and passports. On the other hand, that same technology which is an aid to the American people is a potential risk.

There are a number of technologies that DOD is evaluating for virtual operating systems. They permit the possibility that if there would be a potential threat to the computer system, there would be a refresh of the image of that computer on its next use so that the regular work could go forward. And that is just one of many techniques that we try to work with the Department of Defense on.

Mr. CONNOLLY. I would ask unanimous consent that Mr. Lentz be allowed to answer. My time is up. But if we could just hear the Department of Defense response, if that is acceptable?

Ms. WATSON. Go ahead.

Mr. CONNOLLY. I thank the Chair.

Mr. LENTZ. We completely agree that network resiliency, the ability of our network to be able to withstand and maintain continuity of operations under any form of attack, is a very high priority of ours. We are designing in every day as many measures as possible to ensure that from the top secret sensitive networks to our command and control secret networks we can withstand that kind of sophisticated attack. So we are investing as much as we can to harden that network to do that.

I will say that the growth, as I said, of technology and the escalation of the threat pose a significant challenge to us every single day. We must continue to invest and leap ahead with technologies to stay further ahead of our adversaries instead of just keeping pace with them.

Ms. WATSON. Mr. Cuellar.

Mr. CUELLAR. Thank you, Madam Chair. I think we understand the threats that we are seeing now have been increasing by large numbers. For example, the Department of Homeland Security reported in 2007 that they had received about 18,000 cyber related incidents. The Department of Defense, according to GAO the Department of Defense had received approximately 6 million scans or probes daily from unidentified areas. The Department of Energy, the Los Alamos National Laboratory reported receiving an estimated 10 million probes of its classified systems per month to 2007. I think we have seen even congressional offices that have been subject to some of these attacks also.

I guess one of my questions has to do with lessons learned and what cooperation, communication we have with the different agencies. What best practices are we learning from each other?

Just looking at body language, and I am probably wrong, do you all know each other? Do you talk?

Mr. STREUFERT. Yes.

Mr. LENTZ. Constantly.

Mr. CUELLAR. But do you all work on a professional basis in the sense of this is what we learned, this is what has happened in the State Department, this is what has happened at the Defense Department?

Mr. STREUFERT. Yes.

Mr. CUELLAR. What are the lessons learned that you can tell us that we can share and that the Intelligence Committee or the intelligence community can share with each other? I am sure each agency is learning something on those cyber attacks and how we defend each other, but how do you share that with another agency? It might be that somebody is learning something that could help another agency.

Mr. LENTZ. One of the things that has been a huge priority of ours over the last several years, as you stated in your statistics you said earlier, is the pace by which our network is being scanned. The immensity of that threat is such that our intelligence agencies and our law enforcement agencies are richly connected these days sharing information. From our Joint Task Force for Global Network Operations within the Department of Defense to the Defense Cyber Crime Center, which is our front door for our defense industrial base FE

Mr. CUELLAR. By the way, let me interrupt. GAO reported in 2007 that you all had 6 million unauthorized probes and scans but I think in your testimony you referenced 360 million.

Mr. LENTZ. That is correct.

Mr. CUELLAR. So did it increase from 6 million to 360 million?

Mr. LENTZ. That is correct. That reflects several things.

One, it just reflects, as the chairwoman said, the immensity of the threat. The threat is increasing exponentially. The amount of individuals and machines, what we call in our techie parlance botnets, that are out there, machines pinging the network, probing our network, has grown exponentially.

In addition, we have better sensoring technology within our network now versus 2006. It is now able to allow us to better understand and better have knowledge of these probes and scans that are occurring on our network.

Also, our Computer Emergency Response Teams are now working very much closely together. They collect these statistics that are now reported up, which is what reflected in the more updated report.

That goes to the heart of your very good question. All these centers are working together to be able to share information. The one challenge that we have is protecting information and not letting it out as fast as possible. That is a cultural issue that must be dealt with. That is one that I think is probably the biggest Achilles heel that we have.

We need to have law enforcement and the intelligence community make sure that they open up information as fast as possible because we are talking about real time threats that therefore need real time responses and situation awareness. So we therefore are all learning from each other to deal with that.

Mr. CUELLAR. But what protocols do you all have in place that gets you to provide your lessons learned to, let us say, the gentleman next to you from the State Department? What are the protocols?

Like you were saying, it is moving so quickly. There is a scan and a probe here, and there is something new here. How do we share that? What protocols do we have in place to provide that communication and coordination with other Federal agencies?

Mr. STREUFERT. Congressman, there are things happening on many different levels, beneficially simultaneously. Perhaps what we can learn from this is that we need to get better and better.

These include daily video conferences that are held between the key components of the Government.

Mr. CUELLAR. Does that include Homeland Security?

Mr. STREUFERT. Yes.

Mr. CUELLAR. OK. Thank you.

Mr. STREUFERT. The regular interactions between US-CERT and the civilian agencies are very active. We are discussing signatures in particular threats, responding to things like the recent Conficker and a number of the other threats.

At the State Department, we have a unit which analyzes threats. Because we are members of a country team and have so many locations overseas at embassies and consulates, we are available to assist them if there is identification of a particular problem and they ask about it. We can proactively reach in their direction.

All of these I think are beginnings of an effort where we as a country, if we can become the strongest team among nations, we will do the best in a very rapidly evolving area.

Mr. CUELLAR. I want to thank both of you and the men and women who work with you. I know the future challenges are just amazing. So I really appreciate the work that you all do. Thank you.

Ms. WATSON. I want to thank the panel for your testimony. There are a couple of things we would like to set up a classified briefing about. We will get together with you to determine the time. I think there is far more information that we need to know as part of this hearing or subsequent to this hearing. So we will be in touch with you.

That is the bell that says we have three bills on the floor to vote on. I will dismiss this panel. Thank you very much. You may be dismissed now.

Mr. BILBRAY. Madam Chair, before they are dismissed I would just ask one thing. There is this big issue, to followup on my colleagues, that is the issue that was brought up by the Center for Strategic and International Studies and the concept of having a coordinator in the White House for oversight on all of these agencies. I would ask that you respond in writing specifically to your concerns or your support or whatever you have about the concept of having a designated person in the White House itself to be able to coordinate this.

I appreciate my colleagues bringing up this issue because those firewalls and all the problems we had in 9/11, we are seeing we have the same problems here.

Ms. WATSON. Without objection, we will ask for the committee to raise that question. We will ask for responses as soon as possible.

With that, we will dismiss. We will recess this committee hearing. We will come back, I would say, it would be close to 4 p.m. for panel II. Sorry for the break but we need to get to the floor. Thank you so much for your testimony.

[Recess.]

Ms. WATSON. I would like to invite our second panel of witnesses to come forward. You are already in your seats. It is the policy, as you know, of this committee to swear in all witnesses before they testify. I would like to ask all of you to please stand and raise your right hands.

[Witnesses sworn.]

Ms. WATSON. Thank you. You may be seated. Let the record reflect that the witnesses answered in the affirmative. Now I will take a moment to introduce our distinguished panelists.

Mr. Gregory Wilshusen serves as the Director of Information Security Issues at GAO. His work involves examining Federal information security practices and trends at Federal agencies. He is GAO's leading expert on FISMA implementation.

James Andrew Lewis directs the CSIS Technology and Public Policy Program. He is a Senior Fellow and most recently served as Project Director of the CSIS Commission on Cybersecurity for the 44th Presidency. Before joining CSIS, he was a career diplomat who worked on a range of national security issues during his Federal service, including several bilateral agreements on security and technology.

Lieutenant General Harry D. Raduege retired after 35 years in the U.S. military where he last served as the Director of the Defense Information Systems Agency. He also served as co-chair of the CSIS Commission of Cybersecurity for the 44th Presidency.

Mr. Marcus Sachs is the Director of the SANS Internet Storm Center, an all volunteer Internet early warning service sponsored by the SANS Institute in Bethesda, MD. His professional experience includes a 20 year military career as an Officer in the U.S. Army followed by 2 years of Federal civilian service at the White House as part of the National Security Counsel and at the U.S. Department of Homeland Security.

Then we have Liesyl I. Franz. She is the Vice President for Information Security and Global Public Policy at TechAmerica. Prior to her current position, she worked at the Department of Homeland Security and in Government Relations for EDS.

Now, I will ask that each one of the witness please give a brief summary of your testimony. Keep this summary, if you can, under 5 minutes in duration because your complete written statement will be included in the hearing record.

Mr. Wilshusen, please proceed.

STATEMENTS OF GREGORY WILSHUSEN, DIRECTOR INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; JAMES ANDREW LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; MARCUS H. SACHS, DIRECTOR, SANS INTERNET STORM CENTER, SANS INSTITUTE; LIEUTENANT GENERAL HARRY D. RADUEGE, JR., RETIRED, CO-CHAIRMAN, CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY; AND LIESYL I. FRANZ, VICE PRESIDENT, INFORMATION SECURITY AND GLOBAL PUBLIC POLICY, TECHAMERICA

STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Chairwoman Watson, thank you for the opportunity to participate in today's hearing on the threats, vulnerabilities, and challenges in securing Federal information 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. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained cyber-based attacks against the United States that continue to pose significant risks to systems and to the operations and critical infrastructures that they support.

Cyber threats to Federal systems and cyber-based critical infrastructures are evolving and growing. These threats can be intentional or unintentional, targeted or non-targeted. They can come from a variety of sources such as foreign nations engaged in espionage and information warfare, criminals seeking monetary gain, hackers and virus writers proving their mettle, and disaffected employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal.

Cyber exploitation activity has grown more sophisticated, more targeted, and more serious. Perhaps reflective in part of the evolving and growing nature of these threats to Federal systems, the number of incidents reported to US-CERT tripled during fiscal years 2006 through 2008 from about 5,500 to over 16,800 incidents. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breeches.

These factors highlight the need for effective security policies and practices. However serious and widespread, control deficiencies and vulnerabilities continue to place Federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at the risk of inappropriate disclosure, and critical operations at risk of disruption.

Over the past several years, GAO has made hundreds of recommendations to assist agencies in countering cyber threats, mitigating identified vulnerabilities, and strengthening security controls over Federal information systems. Effective implementations of these recommendations will help agencies to prevent, limit, and detect unauthorized access to computerized networks and systems; help ensure that only authorized users can read, alter, or delete data; better manage the configuration of security features for hardware and software; assure that changes to those configurations are systematically controlled; better plan for contingencies which can prevent significant disruptions of computer-dependent operations; and to fully implement an agency-wide information security program that provides protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, or modification of its information and systems. This includes those operated by contractors.

Agencies have implemented or are in the process of implementing many of our recommendations. Nevertheless, agencies will continue to face significant challenges in securing their systems and information going forward. For example, the complexity of highly diverse, dispersed, and interconnected Federal computing environments; the preponderance of defective software; the increasing reliance on contractors for operational IT support; and the emergence of new technologies, threats, vulnerabilities, and business practices will continue to challenge the abilities of agencies to sufficiently safeguard their information technology resources.

To help address these and other challenges, sustained commitment, oversight, and improvements to the national cybersecurity strategy are needed to strengthen Federal information security. Chairwoman Watson, this concludes my opening statement.

I will be happy to answer questions at the appropriate time.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Government Management, Organization, and Procurement; House Committee on Oversight and Government Reform

For Release on Delivery
Expected at time 2:00 p.m. EDT
May 5, 2009

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-09-661T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

May 5, 2009

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

Why GAO Did This Study

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 maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

GAO was asked to describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. To do so, GAO relied on its previous reports and reviewed agency and inspectors general reports on information security.

What GAO Recommends

In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-09-661T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal, and cyber exploitation activity has grown more sophisticated, more targeted, and more serious. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. In the absence of robust security programs, agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. These developments have led government officials to become increasingly concerned about the potential for a cyber attack.

According to GAO reports and annual security reporting, federal systems are not sufficiently protected to consistently thwart cyber threats. Serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. For example, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, and information, and weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. Agencies also did not always configure network devices and service properly, segregate incompatible duties, or ensure that continuity of operations plans contained all essential information. An underlying cause for these weaknesses is that agencies have not yet fully or effectively implemented key elements of their agencywide information security programs. To improve information security, efforts have been initiated that are intended to strengthen the protection of federal information and information systems. For example, the Comprehensive National Cybersecurity Initiative was launched in January 2008 and is intended to improve federal efforts to protect against intrusion attempts and anticipate future threats. Until such opportunities are seized and fully exploited and GAO recommendations to mitigate identified control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain vulnerable.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the threats, vulnerabilities, and challenges in securing federal information 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 maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

In my testimony today, I will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. In preparing for this testimony, we relied on our previous reports on federal information security. These reports contain detailed overviews of the scope and methodology we used. We also reviewed inspectors general (IG) reports on information security, analyzed performance and accountability reports for 24 major federal agencies,[1] and examined information provided by the U.S. Computer Emergency Readiness Team (US-CERT) on reported security incidents.

We conducted our work in support of this testimony during April and May 2009, in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[1] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. 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, deliver services to the public, and account for their resources without these information assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their information and information systems. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets. For example:

- Resources, such as federal payments and collections, could be lost or stolen.
- 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, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Federal Systems and Infrastructures Face Increasing Cyber Threats

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. In September 2007, we reported[2] that these threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual attacks a specific system or cyber-based critical infrastructure. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software[3] is released on the Internet with no specific target.

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.[4] The Federal Bureau of Investigation has identified multiple sources of threats to our

[2] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

[3] "Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

[4] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

nation's critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation's information systems and cyber infrastructures.

Table 1: Sources of Cyber Threats

Threat source	Description
Foreign nations	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potentially disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[a]
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a] Prepared statement of Dennis Blair, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 12, 2009.

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported,[5] the

[5] GAO, *Cybercrime: Public and Private Entities Face Challenges is Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can more easily remain anonymous.

Table 2 identifies the types and techniques of cyber attacks that are commonly used.[6]

Table 2: Types and Techniques of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering even occurs, such as terminating the programmer's employment.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected files is loaded into memory, allowing the virus to infect other files. Unlike the computer worms, a virus requires human involvement (usually unwitting) to propagate.

[6] GAO-07-705 and GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection,* GAO-04-321 (Washington, D.C.: May 28, 2004).

Type of attack	Description
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
War-dialing	Simple program that dial consecutive phone numbers looking for a modem.
War-driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be sued as a delivery mechanism for malicious software and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial information from the sea of internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO.

Government officials are increasingly concerned about the potential for a cyber attack. According to the Director of National Intelligence,[7] the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical infrastructures. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of IT have moved overseas, the threat will continue to grow. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. For example, the Director of National Intelligence also stated that, in August 2008, the Georgian national government's Web sites were disabled during hostilities with Russia, which hindered the government's ability to

[7] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

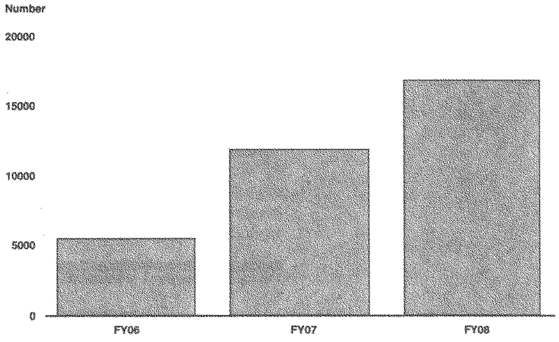
communicate its perspective about the conflict. The director expects disruptive cyber activities to become the norm in future political and military conflicts.

Reported Security Incidents Are on the Rise

Perhaps reflective of the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2008



Source: GAO analysis of US-CERT data.

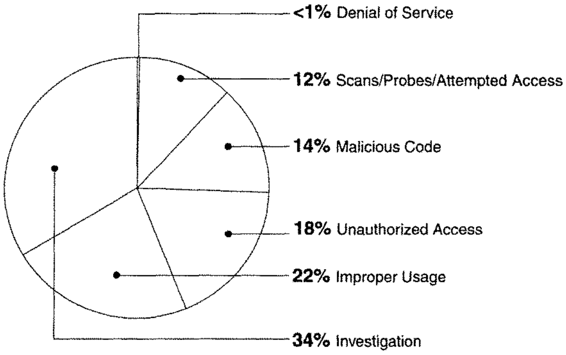
Incidents are categorized by US-CERT in the following manner:

- Unauthorized access: In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- Denial of service: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.
- Malicious code: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
- Improper usage: A person violates acceptable computing use policies.

- Scans/probes/attempted access: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- Investigation: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 2, the three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access, improper usage, and investigation.

Figure 2: Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category



Source: GAO analysis of US-CERT data.

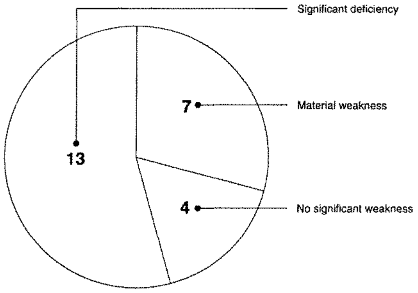
Vulnerabilities Pervade Federal Information Systems

The growing threats and increasing number of reported incidents, highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information were either a significant deficiency or a material weakness for financial statement reporting (see fig. 3).[8]

[8] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 3: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2008.

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example:

- We reported in September 2008[9] that although the Los Alamos National Laboratory (LANL)—one of the nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources. As a result, sensitive information on the network—including unclassified controlled nuclear information, naval nuclear propulsion information, export control information, and personally identifiable information—were exposed to an

[9] GAO, *Information Security: Actions Needed to Better Protect Lost Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

unnecessary risk of compromise. Moreover, the risk was heightened because about 300 (or 44 percent) of 688 foreign nationals who had access to the unclassified network as of May 2008 were from countries classified as sensitive by the Department of Energy, such as China, India, and Russia.

- In May 2008[10] we reported that the Tennessee Valley Authority (TVA)— a federal corporation and the nation's largest public power company that generates and transmits electricity using its 52 fossil, hydro, and nuclear power plants and transmission facilities—had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures. Both its corporate network infrastructure and control systems networks and devices at individual facilities and plants were vulnerable to disruption. In addition, the interconnections between TVA's control system networks and its corporate network increased the risk that security weaknesses, on the corporate network could affect control systems networks and we determined that the control systems were at increased risk of unauthorized modification or disruption by both internal and external threats. These deficiencies placed TVA at increased and unnecessary risk of being unable to respond properly to a major disruption resulting from an intended or unintended cyber incident, which could then, in turn, affect the agency's operations and its customers.

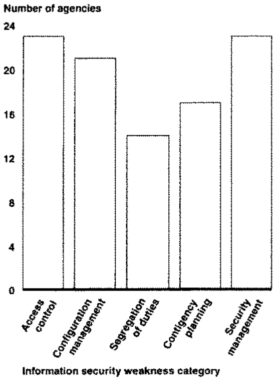
Weaknesses Persist in All Major Categories of Controls

Vulnerabilities in the form of inadequate information system controls have been found repeatedly in our prior reports as well as IG and agency reports. These weaknesses fall into 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 security features for hardware and software are identified and implemented and that changes to that configuration are systematically controlled; (3) segregation of duties, which

[10] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

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 4 shows the number of major agencies with weaknesses in these five areas.

Figure 4: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2008



Source: GAO analysis of IG, agency, and prior GAO reports.

Over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. At least nine agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring 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.

In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information necessary to restore services in a timely manner. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program. An agencywide security program, required by the Federal Information Security Management Act[11], provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 23 of 24 major federal agencies had weaknesses in their agencywide information security programs.

[11] *Federal Information Security Management Act of 2002,* Title III, *E-Government Act of 2002,* Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

Due to the persistent nature of these vulnerabilities and associated risks, we continued to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress;[12] a designation we have made in each report since 1997.

Opportunities Exist for Enhancing Federal Information Security

Over the past several years, we and the IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, the White House, the Office of Management and Budget (OMB), and certain federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *Comprehensive National Cybersecurity Initiative*: In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[13] While these initiatives have not been made public, the Director of National Intelligence stated that they

[12] GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[13] The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[14]

- *The Information Systems Security Line of Business*: The goal of this initiative, led by OMB, is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.

- *Federal Desktop Core Configuration*: For this initiative, OMB directed agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by the National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security. The goal of this initiative is to improve information security and reduce overall IT operating costs.

- *SmartBUY*: This program, led by the General Services Administration, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections Initiative*: This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of 50.

[14] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

In summary, the threats to federal information systems are evolving and growing, and federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations, have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. Opportunities exist to improve information security at federal agencies. The White House, OMB, and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Until such opportunities are seized and fully exploited, and agencies fully and effectively implement the hundreds of recommendations by us and by IGs to mitigate information security control deficiencies and implement agencywide information security programs, federal information and systems will remain vulnerable.

Chairwoman Watson, this concludes my statement. I would be happy to answer questions at the appropriate time.

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Charles Vrabel (Assistant Director), Larry Crosland, Neil Doherty, Rebecca LaPaze, and Jayne Wilson.

Ms. WATSON. Thank you.

Mr. Lewis.

STATEMENT OF JAMES ANDREW LEWIS

Mr. LEWIS. Thank you. I thank the committee for the opportunity to testify.

Digital networks provide real economic benefit but the combination of greater reliance on networks and inadequate attention to security has made our Nation vulnerable. My written statement lists a number of publically known incidents that occurred just in the last year.

The failure to secure America's information infrastructure weakens the United States and makes our competitors stronger. The real risk lies is the long term damage to our economic competitiveness and technological leadership. We are everyone's target. Cyber attacks could provide the capability to disrupt key services as in the case of an opponent who accesses a utilities control system. But the immediate problem is the loss of intellectual property and advanced commercial and military technology to foreign competitors.

Right now, attackers have the advantage. The principal threat comes from well financed and innovative opponents. The most skilled are foreign military and intelligence services with immense resources and experience. The first Russian hack of DOD computers, for example, occurred more than 25 years ago. They have been continuing to engage in this sort of activity ever since. These government agencies, however, are almost matched by highly sophisticated cyber criminals who buy and sell tools and data in virtual black markets and who are safe from the threat of prosecution.

The sources of vulnerability are outdated policy and laws and inadequate technologies. The Internet as it is currently configured and governed cannot be secured. If we continue on the course we are on today where we have not learned how to balance efficiency and security, these vulnerabilities will only grow.

The United States has been trying to improve cybersecurity for more than a decade. The last 12 months have seen some progress. The Obama administration has identified cyber security as an important national security issue. But we are still mired in debate.

There are arguments that the Government should only secure its own networks and lead by example. This won't work because we are really all on one big network, Government and private sector, America and foreigners. It is like saying we should tune up half the car and hope that the other spark plugs are inspired.

Some say that since most networks are privately owned, we should rely on the private sector for defense. This is like saying that since most airplanes are private, we should depend on the airlines to defend our airspace. National security is a function that only the Government can perform adequately.

People worry that if we secure our networks, it will damage America's ability to innovate. But more investment in innovation, which I applaud, is pointless if we are only going to share it for free with our foreign competitors.

We need a comprehensive Government-led approach to secure cyberspace. In recognition of this, the CSIS Cybersecurity Commission, which some of us served on, recommended a broad national approach, the creation of a strong White House cyber advisor with clear authorities, and the development of a national security strategy that would use all the tools of U.S. power.

Government policy will determine whether we fail or succeed. Government acquisition rules can create a market for more secure products. A revised FISMA would improve agencies' security and provide a template for the private sector. International engagement, expanded law enforcement, a judicious use of regulatory powers, and investment education and research can change the situation from one where we are losing to one where we are at least holding our own.

The problems we face in cyberspace, espionage, crime, and risk to critical infrastructure, will not go away. But the risks they pose can be reduced by coordinated Government action.

As you know, the administration is struggling to conclude its 60 day review. Ideally, the review will lead to a strong White House cyber advisor. Without this, cybersecurity in the United States will always be underpowered. But with so many different interests involved, there is a risk that the administration will come up with a solution that makes everyone happy. The only people who will benefit from this will be foreign intelligence agencies and cyber criminals.

I thank you for the opportunity to testify. I will be happy to take your questions.

[The prepared statement of Mr. Lewis follows:]

Testimony
Committee on Oversight and Reform
Subcommittee on Management, Organization and Procurement
United States House of Representatives
"Cybersecurity: Emerging Threats, Vulnerabilities and Challenges in Securing Federal Information Systems"
James A. Lewis
Center for Strategic and International Studies
May 5, 2009

I thank the Committee for the opportunity to testify and I would like to begin by apologizing, as I will not have any of the more dramatic prognostications that often accompany a discussion of the emerging threats, vulnerabilities and challenges. My own view is that it is can be a handicap to developing adequate policy to go about saying that the end is near or that tiny bands of hackers can wreak havoc on a scale or September 11 or Pearl Harbor. They cannot, but that is not to say there is no damage being done to the U.S. in cyberspace. My fear is that when we predict the end of the world, and it does not happen, people lose interest or think the problem is not serious yet in some ways it is not an exaggeration to say we are in crisis. Let me give two examples.

At the start of World War Two, a British carrier was caught off the coast of Norway by two German battleships and sunk. How did the Germans know where the carrier would be? The Germans knew because they had broken the British navel code and were listening in on British naval networks. This could happen again, to us instead of the British, as our prospective opponents can access our networks.

At the end of World War Two, the United States had a monopoly on the atomic bomb. The Soviet Union was able to steal the information that had cost the Americans billions of dollars to develop. The Soviets exploded their first bomb a few weeks after the CIA predicted it would take them years to build one. We are experiencing something similar today when foreign opponents can steal technology without even leaving the comfort of their offices. The United States is unwittingly sharing its intellectual property and technological secrets with hackers around the world, at little or no cost to them.

If you were to look for common themes in these incidents, they would be an unwillingness to recognize our own vulnerabilities or admit how deeply we have been penetrated, and a certain belief in our own superiority over our opponents. I still hear people say that America is the internet leader and that our technology is the best. That was possibly true even as late at ten years ago, but is no longer the case. We may still be first among equals but on bad days, I am not even sure about that.

And we have had many bad days. How did we get end up with these problems? First, the effusion of joy that greeted the commercialization of the internet created its own perverse ideology, that government had no role in cyberspace, that it was too slow and too cumbersome and that any intervention would only choke the wonderful flow of innovation. There is some truth to this, but it is not true for public safety or national security. Second, there was a belief that the market would deliver adequate protection. While a well-regulated market is the most efficient way to organize economic activity, the market has always been recognized as inadequate for national security. Even Adam Smith, the 18th Century British economist, wrote in the Wealth of Nations that markets would not provide for national defense. But we have not.

Second, the technology of cyberspace was not designed to be secure. The goal of the early designers was to ensure rapid, efficient connection. They did not worry about trust and authentication of identity. One result is that a system designed for a few thousand scientists in the United States is, after twenty years, now used by hundreds of millions of people around the globe. It is possible that the Internet, as it is currently architected, can never be secure.

Third, the same forces that led to the rapid growth of internet users have also contributed to the rapid growth of internet-based applications in other industry sectors. Our economy has become more efficient and more productive because many functions – from stocking milk in grocery stores or that runs automatic teller machines to the control systems of our electrical grids – now use digital technology and IP based networks.

This is a real advantage. The use of digital network technologies like the internet has given America an advantage over our economic and military competitors. More importantly, the greater use of digital network technologies will accelerate recovery and growth in the future. In the last five years, our economy has become dependent on cyberspace in ways that are not generally recognized and in the future, it will be even more dependent. The question before us is whether we can find a way to use these technologies securely in order to reap their benefits without crippling loss.

The answer to this question, so far, is no. It is not a technological problem, although there are difficult technological problems to solve. It is a political problem. We are on our fourth attempt to improve cybersecurity. In 1998, Presidential Decision Directive 63 order agencies to begin to cooperate to protect critical infrastructure. PDD-63 still shapes policy, but government and commercial networks are no more secure than they were a decade ago. The 2003 National Strategy to Secure Cyberspace laid out a vision for the secure use of cyberspace, but it was crippled by fighting over turf and ideology and ended up being largely an expression of faith that in the private sector. The 2008 Comprehensive National Cybersecurity Initiative is more interesting. While it was not comprehensive, while it faced the usual turf battles and ideological hurdles, and while it was started far too late in the Administration, it contained several serious and useful initiatives. Finally, the Obama administration began its tenure with a sixty-day review of cybersecurity policy conducted by the National Security Council.

What has changed that made the U.S. start to take the threat more seriously? Beginning perhaps five years ago, U.S. dependence on cyberspace became crucial as we wove network technologies deeply into our daily lives and activities. Our opponents realized this and exploited it unmercifully. 2007 was a year of horror for America's defense of cyberspace and the CNCI was a late effort to respond to the crisis.

This sounds dramatic, and it is important to remember that the disaster was an intelligence disaster for government and a financial disaster for businesses, not the sort of story we see in films involving flames, explosions and death. Just because something is hidden from sight does not mean it is not a disaster and a simple listing of the press accounts of the battle in cyberspace since spring of 2007 gives an idea of the scope of the crisis:

-- The Secretary of Defense's unclassified email was hacked by unknown foreign intruders.

-- NASA was forced to block email with attachments before shuttle launches out of fear they would be hacked, and Business Week reported that the plans for our latest space launch vehicles were obtained by unknown foreign intruders.

-- The National Defense University had to take their email systems offline because of hacks by unknown foreign intruders.

--FAA computer systems were hacked and, as the FAA increases its dependence on modern IP-bases networks, the risk of the intentional disruption of commercial air traffic has increased.

-- The Department of Commerce had to take the Bureau of Industrial Security's networks off line for several months. This Commerce Bureau reviews high tech exports and its networks by unknown foreign intruders.

--The Department of State's networks were hacked and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets it would be an act of war, but when it happens in cyberspace, we barely notice.

--The databases of both the Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

-- Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and resecure the networks.

-- Contractors at DHS and DOD had their networks hacked, as a back door into agency systems.

-- The networks of Congressional offices were hacked by unknown foreign intruders. The incident I know about involved offices with an interest in human rights or Tibet.

-- Canadian researchers found a computer espionage system that they attributed to China implanted on the government networks of 103 countries.

-- Estonia and Georgia had their cyber networks attacked by unknown foreign intruders, most likely at the behest of the Russian government. These were more like cyber riots than crippling attacks, and the Estonians responded well, but they created a wave of fear in countries like the U.S. that depend heavily on cyberspace.

-- Cybercrime became the most profitable and least risky form of bank robbery and credit card fraud, costing our economy tens of millions of dollars. If a robber walked into a bank with a gun and stole a million dollars, it would be all over the front page, but in cyberspace, there are only whispers – and there have been a few cybercrime incidents involving losses of a million dollars. A smart cybercriminal has zero chance of being caught and prosecuted.

-- The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

--I am told that American, European and Japanese companies are experiencing significant losses of intellectual property and business information, but this cannot be confirmed in an unclassified setting.

--Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some of my colleagues would go into the new administration and may have thought it might be interesting to read their emails beforehand.

-- And of course, you have seen the Wall Street Journal articles on the vulnerability of our power grid to cyber attack – a vulnerability we are busy increasing - and the intrusions into some F-35 databases by unknown foreign intruders.

All this in a single year, and there are probably some that I have missed and others we have not even found. It is impressive, and I expect that several unknown foreign intruders have received medals and promotions while some cybercriminals in Eurasia have entered the ranks of the rich.

To take a step back, the U.S. faces "asymmetric vulnerability" in cyberspace. We are as good as our opponents when it comes to offense and espionage, but we are also much more dependent on cyberspace than they are and our defenses are too weak. We are a "target-rich environment." Being the richest economy – even after the crash – and the nation with the most advanced military technology means we are number one on everybody's target list for hacking.

The change in cybercrime is one example of how the threat has increased. Cybercriminals are not amateurs, they are not teenagers in a garage in Mendocino. Cybercriminals now include some of the most skilled programmer in the worlds. They are well organized – there are cybercrime websites and chatrooms that are closed to the public, where you can buy advanced hacking tools, rent botnets (collections of zombie computers to use in an attack) or buy credit card data , bank account, and personal information in bulk – when I say bulk I mean in lots of a thousand or ten thousand – the more you buy, the lower the price. Everything cybercriminals can do, the best foreign intelligence and military services can do as well, if not better.

We cannot simply arrest these people in most cases for two reasons. First, attribution is very difficult – this is why the term unknown foreign entity appears so often n the list above. Criminals and attackers exploit the anonymity of the internet and it is a common trick to attack from one country but make it look like the attack came from somewhere else. Second, the most skilful cybercriminals live outside our borders, often in countries that are de facto sanctuaries for cybercrime. They are outside our jurisdiction and these countries will not always cooperate in law enforcement cases. There is an international treaty on cybercrime – the Council of Europe's Cybercrime Convention, but many nations, including China and Russia, have refused to abide by it. If we cannot catch sophisticated cybercriminals, it is even harder to catch intelligence agents who are protected by their governments.

There is no easy solution to this problem but it is not unsolvable. In December 2008, a CSIS Commission on Securing Cyberspace issued a report with a number of recommendations for how to improve the situation. Our two primary recommendations were to establish strong leadership in the White House by providing the President with a single cybersecurity advisor to guide policy and budgets and to develop a truly comprehensive national strategy that used all the tools of American power. Currently, we have neither. Many large agencies have important roles in and left to their own devices, they will not cooperate to the degree that is needed for cybersecurity. Only the White House can provide national the required vision, based on Presidential Strategy and Directives, and ensure policy coordination. To summarize our other recommendations:

-- Create a comprehensive national security strategy for cyberspace that uses all the tools of U.S. power in a coordinated fashion – international engagement and diplomacy; military planning and doctrine, economic policy tools and the involvement of the intelligence and law enforcement communities. A comprehensive strategy must involve engagement with other nations, both our allies and our opponents, to see how much agreement we can reach on securing cyberspace. This will be a long-term process, but it needs to begin now.

--Publish a public doctrine for cyberspace. The President should state publicly that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the U.S. will protect it, using all instruments of national power. This needs to be said clearly and visibly to put our opponents on notice, not buried in a classified document or in some anonymous official report.

--Use regulatory authorities to ensure that the delivery of critical services can continue when we are attacked. The CSIS report identified four sectors – telecommunications, energy, finance and government services – as the most critical for cyberspace. Securing them will active government policies where the government can compel action when necessary to provide for public safety and national security. Public safety and national security are a government mission and cannot be left to voluntary private efforts.

--Mandate strong authentication of identity for both people and devices for access to the networks for telecommunications, energy, finance and government services. Strong authentication of identity for digital networks can significantly improve defense, if it is done in a way that protects privacy and civil liberties.

--Use acquisitions policies and rule to encourage the development and use of products and services that are secure, based on standards and guidelines developed in partnership with industry.

--Build human capital by expanding research, training and education for information technology and cybersecurity.

-- Refocus and strengthen public-private partnerships and focus them on action, not information sharing.

These recommendations lay out a comprehensive approach to cybersecurity, but recommendations are most valuable when they are implemented. This Committee, along with other committees and with the executive branch, have an opportunity to improve cybersecurity in the United States. Improving Federal government security is an important part of this. Oversight to ensure that cybersecurity becomes a priority for the Federal government is crucial. Too often, we hear that an agency will say that its mission – whether it is health care or air traffic control – is more important and cybersecurity is a lesser priority that can be put on hold Congress can help change this.

Federal acquisitions are a vital tool for improving network security. One of the strongest elements of the CNCI was an initiative called the Federal Desktop Core Configuration. This initiative made vendors sell securely configured products to the government. There were some complaints about the FDCC, but this was more about process than the actual policy, and expanding this initiative would markedly improve the security of government networks

Homeland Security Policy Directive-12 required federal agencies to use secure network credential for all of their employees. This would make it harder for anonymous strangers to penetrate government networks. Although all agencies were expected to comply with HSPD-12 by December 2007, only about a third have actually done so.

The Federal Information systems Management Act desperately needs to be modernized. It currently focuses on compliance with written plans and an agencies FISMA score actually tells us nothing about the security of its networks. A draft bill just introduced by Senator Carper in would greatly improve FISMA by focusing it on real security measures. Along with the FISMA bill, draft legislation introduced by Senators Rockefeller and Snow, by Senator Feinstein on data breaches, and by Senator Lieberman and Representative Thompson on securing the electrical grid have all begun the process of providing a sound legislative structure for a new American effort to secure cyberspace.

In addition to the legislative activity, the White House review of cybersecurity policy has concluded and a new policy may be announced shortly. This was a very intense effort that covered an amazing amount of material in a very short time. While few public details have been released, it appears that the White House will play a greater role in organizing and leading cybersecurity policy and ensuring closer coordination among agencies, and that there will be greater attention to international engagement and to relations with the private sector. If the review produces a strong White House cyber advisor with clear authority to set policy and help guide budgets and a commitment to develop a comprehensive strategy the United States can begin to remedy our serious weaknesses in cybersecurity.

I began this testimony by dismissing dramatic scenarios of cyber Armageddon. It may be worth mentioned a few other scenarios that are worth dismissing. We often hear that the Federal government should lead by example and secure its own networks before advising the private sector. This is a recipe for disaster. The Federal responsibility is to provide for the defense of the entire nation. We sometimes hear that the market will provide the innovations we need for security. I myself wrote this in 1996 and I have been waiting 13 years for those innovations – we need to admit that the market will not deliver without incentives an intervention from the government. Sometimes we hear that since the private sector owns and operates most infrastructure, they should lead in securing cyberspace against foreign militaries and intelligence services or highly skilled international criminals, but this is like saying that America's airlines should secure our airspace against foreign air forces An easy rule of thumb is that any argument that was used to undercut the 2003 National Strategy – and all of these arguments were used then - should be discarded in the current debate. We chose weakness in 2003 and have paid for it ever since.

The United States has made better use of cyberspace than our competitors, and this has provided real economic benefits. Our reliance on cyberspace holds the potential for recovery and future growth. We cannot turn away from cyberspace, nor can we afford to forgo the opportunities it will create. However, the combination of greater reliance on cyberspace and inadequate attention to security has left us more vulnerable than our opponents. If this is not changed, United States will see the continued erosion of its power and influence and our prosperity and security will be irrevocably damaged. Congress and the executive branch have the opportunity to avert this outcome if they act decisively and promptly.

I thank you for the opportunity to testify and will be happy to take your questions.

Ms. WATSON. Thank you.
Mr. Sachs.

STATEMENT OF MARCUS H. SACHS

Mr. SACHS. Thank you, Madam Chairwoman. I appreciate the opportunity to appear before the committee to discuss the important topic of cybersecurity and the challenges if securing Federal information systems. The committee's interest in this topic is timely and crucial to the security of our Nation's most sensitive information. My written testimony is fairly detailed so I will just summarize it now by covering most of the main points.

I would like to look back over our shoulders at how we got to this troublesome position we are in today. Decisions made in the 1980's about Government purchases of commercial off the shelf [COTS], computer hardware and software in lieu of expensive, specially hardened systems made sense when most home, business, and Government computer users did not have access to networks but instead relied on floppy disks. That is what we used to call the old sneakernet. This is how we moved and transferred files between computers.

Back in those days, the malicious code inside the Federal Government's desktop computers was primarily in the form of disk-based viruses. They had little fun names like Brain or Concept. They really weren't much more than an annoyance. In fact, back then, to gain access to a Government desktop computer or file server, you generally had to have physical contact with it or you had to have the ability to talk a Government employee into accessing it for you.

Theft of floppy disks, backup tapes, and printer outputs were the methods that were used by our adversaries to steal sensitive information contained on our Government computer systems.

This started to change in the middle 1990's as more organizations connected their computers to the global Internet and threats beyond the borders of the United States began to take advantage of that connectivity. The growth of Government outsourcing and the increasing dependence on Government contractors also added to the problem of protecting sensitive data since information was no longer uniquely stored on Government computers and behind layers of rigid security barriers.

Also in the 1990's the .com explosion happened and the Internet became a common household word. Nuisance viruses and Web site defacements were the weapons that both adolescents and political protestors, as well as others, used to express their views. In fact, we had a string in the late 1990's of hundreds of .gov Web sites that were defaced. It was a very embarrassing situation for cia.gov, Congress.gov, speaker.gov, and whitehouse.gov.

But while these Web site defacements were a very visible sign of the difficulties we faced, a less visible conflict on two fronts was brewing that we continue to deal with today. That is cyber crime and cyber espionage.

In my written testimony, I outline several actions that the Government has already taken since the middle 1990's in terms of new organizations and new partnerships with the private sector. But let me just summarize briefly five items I think we should do to continue making the Internet more secure.

The first is that Government's most important role is truly to set the example. If the Government were to manage its own computer networks in a manner that can be an exemplar for others to follow, then we in the private sector can point to the Government and say, follow them and do as they do.

Second, the Government must use its acquisition powers to improve everybody's ability to secure cyberspace. There was a large effort by the Air Force, OMB, NSA, DISA, NIST, Microsoft, and others to build what today we call the Federal Desktop Core Configuration. That standard can not only be used by the Federal Government but by any organization that uses Windows XP and Windows Vista operating systems. This is the type of leadership we need. It can't stop with just Windows. We need to have all software secured and we can use that procurement angle to do that.

Third, the Government must develop a career field for cyberspace professionals. We are talking about initial entry all the way to senior executives. If we don't immediately address this problem, we will never be able to secure the Federal Government's networks. Security is not about applying just the latest patch or running the latest anti-virus software. It is also about culture and risk management and leadership. It truly is about the people.

Fourth, we need to think about how we view cyberspace and, in particular, how we view the Internet. If we think about industrialism from the 19th century, cyberspace is really industrialism of the 21st century. It is what fuels our economy. We cannot allow it to become a combat zone. We can't let the criminals take it over. We can't let the spies dominate. We need to change this conversation and argue that cyberspace is the cornerstone of America's global leadership and our economic prosperity as we go forward in this century. If we look at cyberspace through the lens of economics, perhaps then we will find some better approaches to secure it.

Fifth, cyberspace exists because of the combined work of the Federal Government and the private sector with the scientists, researchers, investors, and other leaders. It is not the single domain of either Government or the private sector. It must be protected from damage by both parties working in unison. We have come a long way over the past several decades in building strong public/private partnerships. We cannot let those relationships weaken or dissolve.

The last thing I want to mention briefly is that industry has been doing quite a bit of research as well, trying to find out how intrusions happen, how breeches occur. One of the most remarkable reports is this one that Verizon Business has come up with. This is the second year. What it tells us is that almost everything is preventable. These breeches that are costing millions of dollars in credit cards and others are all preventable largely if we just do simple steps. If we follow the rules we have already come up with, this goes away.

It is inexcusable that in 2009 our Nation seems to be unable to prevent our adversaries from breaking into our networks. It is also inexcusable that we continue to run our computer networks as though they are some magical enterprise only understandable by geeks and nerds. Cyberspace does belong to all of us and we are all part of the solution to making it more secure.

Madam Chairwoman, I again appreciate the opportunity to appear before the committee. I look forward to answering any questions.

[The prepared statement of Mr. Sachs follows:]

Testimony of Marcus H. Sachs
Director, SANS Internet Storm Center

Before the House Committee on Oversight and Government Reform,
Subcommittee on Management, Organization, and Procurement

"Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems"

May 5, 2009

Madam Chairwoman and members of the Committee:

Thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing federal information systems. The Committee's interest in this topic is timely and crucial to the security of our nation's most sensitive information. After giving you a very brief background of my professional experience I would like to address the broad subject of securing federal information systems via the lessons I've learned from the perspective of a career military officer and federal civil servant, as the director of the SANS Internet Storm Center, and as a private sector professional working with the national security and emergency preparedness (NS/EP) community here in Washington.

I am a retired United States Army officer, and I spent the second half of my career designing, operating, and defending both tactical as well as strategic military computer networks. My last military assignment was with the Joint Task Force for Computer Network Defense (JTF-CND, now the JTF-GNO) where I was a member of the initial cadre and served for three years. Shortly after retiring from the Army at the end of 2001 I was appointed to the staff of the National Security Council and was part of the team that wrote the National Strategy to Secure Cyberspace.

After we published the strategy in February 2003 I joined the staff of the brand new Department of Homeland Security where I became the Cyber Program Director in the Information Analysis and Infrastructure Protection (IA/IP) Directorate. At first I was the only cyber guy on the staff of DHS, and immediately began trying to find other cyber experts around the Department to leverage into a virtual cyber security team. While building that team I developed the concept of what eventually became the United States Computer Emergency Readiness Team, or US-CERT, which was launched in September 2003 and today has a proposed 2009 budget of over $240 million.

When I left the federal government at the end of 2003, I asked the privately owned SANS Institute if I could direct their Internet Storm Center, a group of cyber security volunteers that I had been affiliated with while in the military and at the White House. The Internet Storm Center is a threat watch and warning organization that has no physical office or operations center, in fact it only exists in cyberspace. It is staffed by over forty volunteer incident handlers around the world and is used by tens of thousands of system administrators, including many in the federal government, as an authoritative source of information about malicious activity online.

In addition to that volunteer work, since leaving government service in 2003 I was employed for three years by SRI International as the deputy director of their Computer Science Laboratory, primarily supporting DHS' cyber security research activities; and since 2007 I have been employed by Verizon as an executive director for national security policy. In 2007 and 2008 I was part of the CSIS Commission on Cyber Security for the 44th Presidency, and chaired two of the Commission's working groups. I will draw upon all of these experiences in my comments to the Committee today.

I would like to start with a look back over our shoulders at how we got to the troublesome position we are in today. Decisions made in the 1980s about government purchases of commercial off-the-shelf (COTS) computer hardware and software in lieu of expensive specially-hardened systems made sense when most home, business, and government computer users did not have access to networks but relied instead on floppy disks (the "sneaker net") to copy and transfer files between computers. At that time, malicious code inside the federal government's desktop computers was primarily in the form of disk-based viruses with names like "Brain" and "Concept" and was not much more than just an annoyance.

In fact, to gain access to a government desktop computer or file server you generally had to have physical access to it, or the ability to talk a government employee into granting the access. Theft of floppy disks, backup tapes, and printer outputs were the methods used by our adversaries to "steal" sensitive information contained on government computer systems. This changed in the mid-1990s as more organizations connected their computers to the global Internet and threats beyond the borders of the United States began to take advantage of the connectivity. The growth of government outsourcing and the increasing dependence on government contractors further added to the problem of protecting sensitive data since information was no longer uniquely stored on government computers, behind layers of rigid security barriers.

Also in the 1990s, the "dot-com explosion" happened, the Internet became a common household word, and millions of government and industry employees wanted to be able to do at work what they were doing at home (and vice-versa) with respect to desktop computing. Compared to today, threats online were generally unsophisticated in the 1990s. Nuisance viruses and website defacements were the common weapons used by both adolescents and political protestors as methods of expression. In fact, the government had to deal with hundreds of embarrassing website security breaches in the late 1990s, including defacements of www.cia.gov, www.congress.gov, www.faa.gov, www.doj.gov, www.senate.gov, www.speaker.gov, www.va.gov, and www.whitehouse.gov.[1] But while the website

[1] http://www.attrition.org/mirror/attrition/gov.html

defacements were a very visible sign of the difficulties the government was facing in meeting the new challenges of cyberspace security, a less visible conflict on two fronts was brewing that we continue to deal with today – organized cyber crime and nation-state cyber espionage.

After the fall of the Soviet Union the United States and other countries expected that the former Soviet countries would rapidly join the ranks of democracy and freedom. We believed that by encouraging capitalism and sharing our industrial know-how, in a short period of time Eastern Europe would be on par with Western Europe and there would be an increase in economic prosperity for all. Unfortunately that scenario did not play out as we expected. Instead, thousands of highly educated Russians, Ukrainians, Romanians and others were left unemployed as the governments shrank in size and new businesses failed. Being a central component of the Soviet political system, organized criminal groups began to fill the void of employment left by the shrinking job market.[2]

The growth of the Internet was an incredible break for these gangs, a "perfect storm" for cyber crime. The Internet offered a way to make money, an opportunity to put bread on the table. These groups fully understood the criminal prospects offered by an expanding and uncontrolled global computer network that has virtually no transaction taxes (and therefore no need for tax evasion), provides anonymous access to nearly everything online, has weak or nonexistent political and national boundaries, where criminal tools are functionally the same as lawful tools, that offers numerous opportunities for money laundering, has little or no cyber law enforcement present, and contains millions of victims that will believe just about anything they see. How could they pass this opportunity by? It did not take long for them to find it.

Between June and October 1994, an organized Russian crime gang successfully transferred $10 million from Citibank to different bank accounts around the world. Known as the "Citibank Caper," this incident was partially responsible for prompting the "Security in Cyberspace" hearings in the U.S. Congress chaired by Sam Nunn. After examining information security risk profiles of hundreds of major companies and several government agencies, the hearings found that computer security complacency was widespread across government, academia, and all economic sectors. Sound familiar? Fifteen years later we have made much progress, but if the same investigation were conducted today we would still find large pockets of complacency and ignorance, especially in those sectors where there is a general feeling that computers and information systems are isolated from the Internet and protected by imaginary barriers.

In fact, the Internet Crime Complaint Center found that in 2008 cybercrime was up 33% from 2007, making last year the worst on record. In 2008, there were over $250 million of reported losses in the United States from cyber crime, compared to $18 million in 2001.[3] Later in my testimony I will talk about what Verizon found by researching several hundred data breaches over the past five years. Criminals are bypassing our strengths and attacking our weaknesses. They know we are investing in security but they are taking advantage of simple mistakes we are

[2] http://www.ncjrs.gov/pdffiles1/nij/187085.pdf
[3] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

making. The fortunate lesson is that those weaknesses and mistakes are fairly easy to identify and fix, and do not cost a lot in terms of resources. All it takes is a willingness to tackle the problem at the senior leader level and not ignore it or delegate it to junior system administrators.

Cyber espionage has followed the same path as cyber crime, and in many cases is technically identical in terms of tools and access methods. During the Cold War and in the centuries prior to it, nations took great risks to recruit and train spies to operate on foreign soil. Today, the Internet has made spying as easy as opening up a web browser and querying a search engine, and has reduced the risk of loss of human life to nearly zero. Why spend hundreds of thousands of dollars to train and equip a spy when surfing to a foreign country's computers provides just as much information at practically no cost? Nearly all countries conduct foreign espionage and Internet access has simply made that process easier. Unfortunately many countries including ours "give away" secrets by allowing open access to research institutions, government contractors, and the government's own networks.

In the late 1990s several US government systems were found to have hidden accounts and large amounts of unauthorized activity. As the investigation[4] developed, more computers and systems outside of the federal government were found to have unauthorized accounts. "Data exfiltration" became the new buzzword, rather than "intrusion" or "unauthorized access." The targets seemed to be large databases that contained atmospheric data, bathymetric data, and other information that took decades to accumulate. The source of the attacks was not clear – the intruders used complex methods to route attacks through multiple compromised computers, and used "drop sites" as collection points for the data being stolen. In no cases were any signs of disruption present. It all appeared to be electronic espionage, a classic case of theft of intellectual property, only via the Internet rather than using microfilm and a spy camera as James Bond would have done.

During the Cold War the activity was clearly centered on US vs. USSR espionage. But in recent years the concern has moved from former Soviet countries to China in terms of espionage directed against the United States. What is unique about China, and which really complicates matters for us, is that the culture in China (and Asia in general) supports academic and scholarly achievement. Many students and professors treat the Internet as an experiment in human communications, and routinely gain access to remote systems or locate bugs in vulnerable software purely for academic purposes. Their findings are published in academic papers, and the researchers move along to the next project. Some, however, have found that there is incredible value in this research and have begun to make a business out of it, selling their findings to governments, criminal groups, and perhaps even terrorists.

A recent example of such a cyber espionage attempt coming from China shows how they gain access. In the spring of 2006, a government system administrator in the United States noticed that many of his users were receiving unexpected e-mails with Microsoft Word attachments

[4] The investigation was called Moonlight Maze

written in Chinese. When opened, Word would crash and sometimes the computer would have to be rebooted in order to function again. The problem was eventually traced to what we call a "zero-day vulnerability" in Word. This means that something was wrong with the software, and the defect allowed for remote access if exploited correctly. Even worse, at the time this was discovered there was no patch for the flaw. Somebody in China figured out how to take advantage of it and launched a targeted email attack against US government computers to gain remote access.

Eventually it was determined that the group behind the attacks was a gang of young Chinese hackers selling information they obtained from US and Japanese computers.[5] The only glimmer of good news in this story is that the ring leader of the Network Crack Program Hacker (NCPH) group, Tan Dailin (aka "Withered Rose" in hacker channels) was recently arrested and faces about seven years of jail time in China.[6]

I'm sure that the Committee is painfully aware of the "Titan Rain" intrusions that were made public over the past few years. Titan Rain was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks were believed to be Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) remains uncertain. The designation "Titan Rain" was changed, and the current name for the attacks is itself classified. The attacks continue to the present day, and are the primary motive behind the Bush administration's Comprehensive National Cybersecurity Initiative launched in 2007.

The intrusions are not just aimed at government computers. In fact, nearly all of the government's prime contractors have been targeted, and many have fallen victim. The most recent account is unnerving – foreign intruders reportedly gained access to the plans for the Defense Department's Joint Strike Fighter program via the computers of a major defense contractor.[7]

In response to rapidly the growing threats in cyberspace, the government has been working hard to keep up with the problem. The "Security in Cyberspace" hearings in the U.S. Congress chaired by Sam Nunn were already mentioned. Shortly after those hearings, and largely in response to the 1995 Oklahoma City bombing the Clinton administration launched a series of initiatives to increase the security of our nation's critical infrastructure, including the soft underbelly of cyberspace. A new organization, the Federal Computer Incident Reporting Center (FedCIRC), was established by NIST in 1996 to bring together resources from the Defense and Energy departments in order to develop a cyber incident response capability for the federal civilian agencies. FedCIRC was transferred to the General Services Administration in 1998, and then was absorbed by DHS in 2003.

[5] http://www.time.com/time/magazine/article/0,9171,1692063,00.html

[6] http://www.thedarkvisitor.com/2009/04/withered-roselaw-done-come-and;got-him

[7] http://online.wsj.com/article/SB124027491029837401.html

Presidential Decision Directive 63, issued in May 1998, correctly identified the risks our nation faced not only in the physical world but also in cyberspace. It specified what sectors of the economy were deemed to be "critical" and set in motion the creation of several new government organizations needed to coordinate the protection of the nation's critical infrastructure, including the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), and a public/private partnership called the Information Sharing and Analysis Center (ISAC).

Today, the NIPC and CIAO are gone, having been absorbed with the FedCIRC into DHS in 2003. The ISAC (singular) never happened, but instead several ISACs (plural) were established by the private sector to work with their government counterparts. About a dozen of the ISACs are still around, serving as a bridge between the private and public sectors in the coordination and dissemination of threat and vulnerability information. Policy coordination bodies, known as "Sector Coordinating Councils" were established as part of Homeland Security Presidential Directive 7 in 2003, and DHS also manages several cross-sector coordination groups including the Cross Sector Cyber Security Working Group and the Industrial Control Systems Joint Working Group. But even with all of the new organizations and an increased interest in sharing critical information between the public and private sectors, intrusions into federal systems continue to grow in the current decade.

The most recent effort to protect government systems is President Bush's Comprehensive National Cyber Security Initiative. Launched in the summer of 2007, and formalized in NSPD-54/HSPD-23, it consists of twelve major projects ranging from the creation of new monitoring systems to limiting the number of gateways between government networks and the public Internet. It also contains efforts to develop a stronger cyber security workforce in the federal government and attempts to strengthen ties between the federal government and the owners/operators of critical infrastructures that depend on computer networks. Earlier this year, President Obama tasked his staff to conduct a comprehensive review of all of the nation's cyber policies in order to develop a roadmap for improvement. The "60-day review" as many call it is not yet public but reportedly calls for a new position at the White House to lead the effort, and recommends changes for several departments and agencies.

The private sector is also engaged and over the past several years has developed and published numerous recommendations concerning the security of cyberspace. I was fortunate to be a member of the Center for Strategic and International Studies (CSIS) Commission on Cyber Security for the 44th Presidency. Our report was published at the end of 2008 and has three major findings: cyber security is a major national security problem for the United States; decisions and actions we take to protect ourselves in cyberspace must respect privacy and civil liberties; and only a comprehensive national security strategy that embraces both the domestic and international aspects of cyberspace will make us more secure. Our commission had several recommendations for the federal government including: create a comprehensive national strategy for cyberspace, lead from the White House, reinvent the public-private partnership, modernize authorities, use acquisition policy to improve security, and do not start over.

I would like to go beyond those recommendations with some of my own observations and thoughts. First, the government should lead by setting the example. Securing an organization's corner of cyberspace is hard. It normally does not generate revenue (unless you are selling security services) and it is difficult to show senior organizational leadership why it is important. If the government was to manage their own computer networks in a manner that can be an exemplar for others to follow, we in the private sector can point to the government and say, "follow them, do as they do." But when government computer systems are easy to break into and offer our adversaries an easy opportunity for theft of our nation's secrets, it is easier to say "don't follow them, don't do as they do." We need not only the government as a whole to lead by example, but we need an organization inside the government to take an internal lead and set the example for the rest of government to follow.

Second, the government must use its acquisition powers to improve everybody's ability to secure cyberspace. The story about the Air Force's use of procurement policy to insist that Microsoft develop a more secure version of the Windows operating system must be told over and over.[8] Today, thanks to the efforts of the Air Force, OMB, NSA, DISA, NIST, Microsoft, and others there is a very strong "Federal Desktop Core Configuration" standard that can be used not only by the federal government but by any organization that uses the Windows XP or Windows Vista operating systems.[9] But it cannot stop there. We need more secure software from all vendors, and we need the federal government to continue to use its acquisition and procurement policies to drive that effort.

Third, the federal government must develop a career field for cyberspace professionals, from initial entry all the way to SES. There are a few cyber scholarship opportunities available for college students, and we do a very poor job of managing their careers. We are too reliant on contractors and temporary employees to fill in gaps where we need career civil servant professionals. If we do not immediately address this problem, we will never be able to secure the federal government's networks. Security is not all about applying the latest patch, running updated antivirus software, or installing a new firewall. It is about culture, risk management, and leadership. Without a trained and dedicated workforce and leaders who are willing to lead through personal involvement in mandating cyber security in their organizations, we are sitting ducks for continued abuse coming from our adversaries.

Fourth, we must rethink the way we view cyberspace and in particular the Internet. It started as an experiment, a proposed way to link together expensive mainframe computers so that researchers and strategic military planners could share computing resources via the nation's communication backbones. For a couple of decades, the general public was largely unaware of its existence, but in academic circles it was mesmerizing and every university wanted to be a part of it. The military understood its importance too, and spent millions of dollars to build computer networks connecting nearly every military base world-wide. When general society was invited to participate, new uses emerged that today include a multitude of audio, video,

[8] http://hsgac.senate.gov/public/_files/042809Paller.pdf, pp. 4-5
[9] http://fdcc.nist.gov

and data services. Cyberspace is everywhere, we depend on it, and our nation cannot do without it.

But we cannot let the future of the Internet be driven by military, espionage, or criminal forces. It's important to maintain our military defenses, but a strong desire to use cyberspace as a battlefield is harmful to what it's really good for – becoming the essence of the nation's economic recovery. Like industrialism in the 19th century, cyberspace today is what fuels our economy. We cannot let it become a combat zone, and we certainly cannot let the criminals or spies take it over either. We need to change the conversation and argue that cyberspace is the cornerstone of America's global leadership and economic prosperity in this century. By looking at cyberspace through the lens of economics, we might find better approaches to securing it.

Fifth and finally, cyberspace exists because of the combined work of government and private sector scientists, researchers, investors, and leaders. It is not the single domain of either government or the private sector and must be protected from damage by both parties working in unison. We have come a long way over the past several decades in building strong public-private partnerships and we cannot let those relationships fall apart. It has been long understood in the physical world that defense of private property begins with the property owner, but in accordance with laws provided by the government. While the federal government provides for a national defense, it depends on private property owners to adequately secure their property from theft, as well as from natural threats such as wind, fire, or floods. It also depends on the private sector to provide materiel, labor, know-how, and innovation in order to adequately protect the nation from foreign adversaries. In cyberspace we should think the same way, with the federal government oriented on making and enforcing laws that permit a private property owner to adequately defend that property, while working with the private sector to provide a "national defense" oriented externally against threats coming from beyond our shores.

The last subject I would like to address is what Verizon's investigation teams found when they examined forensic information from several hundred data breaches over the past five years.[10] The latest report just came out last week and the findings can serve as a roadmap for where the federal government and others should be investing resources if they want to reduce or eliminate data breaches. In 2008 alone, the Verizon team investigated 90 confirmed data breaches that encompass an astounding 285 million compromised records.

The investigations showed that as expected, most of the breaches were from external sources, but a third of the breaches originated in trusted third-party connections that were used as a conduit to break into the victim's network. Nearly 90% of the breaches were preventable if system administrators had not made simple configuration mistakes, and over 80% of the victims were not compliant with the Payment Card Industry (PCI) standards. Other bothersome observations include the fact that in over half of the cases it took days, weeks, or months for the attacker to figure out how to break in. That's a lot of time for early detection. But in spite

[10] http://www.verizonbusiness.com/worldwide/products/security/risk/databreach

of that, in over 75% of the cases it took weeks or months after the breach occurred and data was stolen for the victim to figure out that they had been compromised. To make it worse, in nearly 80% of the cases it took another several days or weeks to stop the attack after it was discovered.

The bottom line is that nearly all intrusions are preventable and that we can make a lot of this problem go away (or at least make it harder for the bad guys) by following best practices and educating our users. It's inexcusable that in 2009 we seem to be unable to prevent our adversaries from breaking into our computer networks. It's also inexcusable that we continue to run our computer networks as though they are some magical enterprise only understandable by geeks and nerds. Cyberspace belongs to all of us, and we are all part of the solution to making it more secure.

Madam Chairwoman and members of the Committee, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing federal information systems. I look forward to answering any questions you may have.

Ms. WATSON. Thank you.

Mr. Raduege.

STATEMENT OF LIEUTENANT GENERAL HARRY D. RADUEGE, JUNIOR

General RADUEGE. Chairwoman Watson, Ranking Member Bilbray, and members of the subcommittee, thank you for the opportunity to join in today's hearing to discuss efforts to protect our Nation from current and emerging cyber threats and vulnerability of our Nation's critical infrastructures to exploitation, attack, and disruption.

Relentless and continuing cyber intrusions into Federal Government systems, defense industrial base companies, and supporting critical infrastructures continue to pose serious national security risks to our Nation. While I understand the main focus of this hearing is centered primarily on Federal Government systems, I would also point out that cyber crime is an escalating problem that affects all citizens and businesses.

The cyber threat has no boundaries. In fact, a variety of studies have identified the serious implications of cyber crime focused on stealing financial and personal information and the tremendous economic impact of this profit driven activity. The problem of cyber threats affects not only our national security but also our economy and the privacy of all our citizens.

Cybersecurity is an issue that is front and center from a public policy perspective as the new administration grapples with how to handle an overall national cyber strategy. Various reports have come out over the past several months, including the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. I was privileged to co-chair this Commission. This important effort provided findings and recommendations to secure cyberspace for the country and to help guide policymaking. It called for immediate action to create a comprehensive national security strategy for cyberspace.

The new administration has cybersecurity high on its agenda and is making a serious effort to take what has already been done and improve our national cyber posture. While I am hopeful, there is still much to be done. Improving the security of our Federal networks and Nation's digital infrastructures will be a long term effort. But immediate, focused attention on this significant challenge is absolutely critical.

As our Commission report noted, cybersecurity is now a major national security problem for the United States. In response, we need to focus all tools of national power, diplomatic, economic, military, intelligence gathering, and law enforcement, on this critical issue.

I would like to briefly highlight three challenges facing the Federal Government's information systems and critical cyber infrastructure assets.

First, despite the increased attention by this administration and the 60 day cybersecurity review led by Ms. Melissa Hathaway, it is imperative that the Federal Government be organized properly for the emerging threats and vulnerabilities in securing Federal information systems. Currently, our networks and systems are under continuous and relentless cyber assault. We are losing a significant amount of personal and sensitive data every day. Even worse, we are losing competitive advantage globally.

The Federal Government must become a model for cyber security and it must start by securing our networks and information as quickly as possible. While efforts like the Comprehensive National Cybersecurity Initiative will bear fruit over time, we need leadership throughout the Federal Government to make this a focus area. Securing our networks and protecting information on those networks is an important matter of public trust. Government must be well organized to lead.

Second, raising the level of education and awareness of the seriousness of the threats is imperative. Those who work in the cybersecurity business clearly understand the magnitude of the problems and are very concerned about the current state of affairs. However, for many in both Government and industry the threats are abstract, the implications are not fully understood, and their ability to help is unclear. An aggressive outreach and awareness campaign is needed in creating a cybersecurity mindset to raise the level of knowledge of Federal leaders and the work force that our Nation is constantly under cyber attack. We need to ensure that every person who logs onto a system connected to the Federal enterprise is properly educated and trained to protect the information with which they have been entrusted.

Third, there is a need for clearly delineated roles and responsibilities within the Federal Government for cybersecurity. While the administration is focused on addressing this concern, it is critical to ensure a successful cybersecurity strategy. A properly structured and resourced organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and our Nation's international allies to address incidents against critical cyber infrastructure systems and functions is essential.

In summary, our Nation and, in particular, Federal networks and systems are under relentless cyber assault. While many good efforts are underway, much more in needed, faster. The Federal Government must focus on understanding cyber risk and take appropriate action to secure its networks and become a model for others. Today, that is not the case. We also must change the culture of the Federal work force by raising and maintaining awareness of cyber threats that are focused on gaining access to our networks every day, 24 hours a day. Finally, we must clearly identify who is in charge with respect to Federal cybersecurity.

Madam Chair, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

[The prepared statement of General Raduege follows:]

Opening Statement by Harry D. Raduege, Jr., Lt. General, USAF (Ret)
Chairman of Deloitte Center for Network Innovation

Subcommittee on Government Management, Organization and Procurement
"Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems"
Tuesday, May 5, 2009

Chairwoman Watson, Ranking Member Bilbray, and Members of the Subcommittee, thank you for the opportunity to join in today's hearing to discuss efforts to protect our nation from current and emerging cyber threats and vulnerability of our nation's critical infrastructures to exploitation, attack, and disruption. Relentless and continuing cyber intrusions into Federal government systems, defense industrial base companies, and supporting critical infrastructures continue to pose serious national security risks to our nation. And while I understand the main focus of this hearing is centered primarily on Federal government systems, I would also point out that cyber crime is an escalating problem that affects all citizens and businesses. The cyber threat has no boundaries. In fact, a variety of studies have identified the serious implications of cyber crime focused on stealing financial and personal information and the tremendous economic impact of this profit-driven activity. The problem of cyber threats affects not only our national security but also our economy and the privacy of all our citizens.

Cybersecurity is an issue that is front and center from a public policy perspective as the new Administration grapples with how to handle an overall national cyber strategy. Various reports have come out over the past several months, including the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. I was privileged to co-chair this Commission. This important effort provided findings and recommendations to secure cyberspace for the country and to help guide policy-making. It called for immediate action to create a comprehensive national security strategy for cyberspace. The new Administration has cybersecurity high on its agenda and is making a serious effort to take what has already been done and improve our national cyber posture. While I am hopeful, there is still much to be done. Improving the security of our Federal networks and nation's digital infrastructures will be a long-term effort, but immediate focused attention on this significant challenge is absolutely critical. As our Commission report noted, cybersecurity is now a major national security problem for the United States. In response, we need to focus all tools of national power – diplomatic, economic, military, intelligence gathering, and law enforcement -- on this critical issue.

I would like to briefly highlight three challenges facing the Federal government's information systems and critical cyber infrastructure assets.

First, despite the increased attention by this Administration and the 60-day cybersecurity review led by Ms. Melissa Hathaway, it is imperative that the Federal government be organized properly for the emerging threats and vulnerabilities in securing Federal information systems. Currently, our networks and systems are under continuous and relentless cyber assault. We are losing a significant amount of personal and sensitive data every day. Even worse, we are losing competitive advantage globally. The Federal government must become a model for cybersecurity, and it must start by securing our networks and information as quickly as possible. While efforts like the Comprehensive National Cybersecurity Initiative will bear fruit over time, we need leadership throughout the Federal government to make this a focus area. Securing our networks and protecting information on those networks is an important matter of public trust; and government must be well organized to lead.

Second, raising the level of education and awareness of the seriousness of the threats is imperative. Those who work in the cybersecurity business clearly understand the magnitude of the problems and are very concerned about the current state of affairs. However, for many in both government and industry, the threats are abstract, the implications are not fully understood, and their ability to help is unclear. An aggressive outreach and awareness campaign is needed in creating a cybersecurity mindset to raise the level of knowledge of Federal leaders and the workforce that our nation is constantly under cyber attack. We need to ensure that every person who logs onto a system connected to the Federal enterprise is properly educated and trained to protect the information in which they have been entrusted.

Third, there is a need for clearly delineated roles and responsibilities within the Federal government for cybersecurity. While the Administration is focused on addressing this concern, it is critical to ensure a successful cybersecurity strategy. A properly structured and resourced organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and our nation's international allies to address incidents against critical cyber infrastructure, systems, and functions, is essential.

In summary, our nation and, in particular, Federal networks and systems are under relentless cyber assault. While many good efforts are underway, much more is needed, and faster. The Federal government must focus on understanding cyber risk and take appropriate action to secure its networks and become a model for others. Today, that is not the case. We also must change the culture of the Federal workforce by raising and maintaining the awareness of cyber threats that are focused on gaining access to our networks every day, 24 hours a day. And finally, we must clearly identify "who's in charge" with respect to Federal cybersecurity.

Madame Chair, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

Ms. WATSON. Thank you.

Ms. Franz.

STATEMENT OF LIESYL I. FRANZ

Ms. FRANZ. Madam Chair, thank you and Ranking Member Bilbray for the opportunity to appear today and to provide the technology industry's perspective on cybersecurity and securing Federal information systems.

Today's highly interconnected environment presents great opportunities to innovate and create economic prosperity, but it also presents challenges as my fellow witnesses have clearly descried today. But let me highlight two clear trends. First, the attackers are more sophisticated and increasingly able to target their attacks more directly and efficiently. Second, the insider threat is a prevalent concern that illustrates that technology alone is not the only problem or the only solution. It is people and processes as well. We see three key elements to better securing Government information systems.

First, the President should act quickly to appoint a senior cybersecurity advisor that reports directly to the President. He or she should have the authority needed to develop, coordinate, and execute upon the President's cybersecurity priorities in partnership with Congress, industry, and other stakeholders. A cybersecurity advisor reporting directly to the President is the surest way to muster the perspective and authority necessary to protect the United States in cyberspace.

Crucial elements to making progress are a strategy that includes ensuring senior level attention to cybersecurity as a national priority, developing a comprehensive and coordinated strategy across the Government in partnership with the private sector, and integrating cybersecurity into the deliberation on the issues of highest national concern such as economic prosperity and technological innovation.

We commend the President for initiating a 60 day cybersecurity review and its consultative process. We look forward to its release.

Second, we need to reform the Federal Information Security Management Act. We were a big champion of FISMA when it was enacted in 2002 but it should evolve to meet today's demands, moving beyond compliance to more effective security measures. In previous testimony before this committee's Subcommittee on Information Policy, Census, and National Archives, we described six areas for improvement. We provide that for your reference and look forward to working with you on new FISMA reform proposals.

Third, we must strengthen the public/private partnership to address both strategic and operational concerns both here at home and globally. That partnership is critical to addressing cybersecurity risks throughout the ecosystem which will positively impact Federal systems as well. We support the partnership model that was established in the National Infrastructure Protection Plan. The NIPP is not perfect but it has improved over time and it provides a framework for strategic and operational collaboration going forward.

A key component is the IT Information Sharing and Analysis Center, which is the operational focal point of the IT sector. There are similar ISACs, or Information Sharing and Analysis Centers, for other sectors. We continue to recommend two-way information sharing and analysis about specific threats between the industry and Government, and the colocation of Government and industry experts working side by side on a continuous basis to address those threats.

Industry is playing a key role in cybersecurity and critical information infrastructure protection. Allow me to outline it. We participate in the IT ISAC. We participate in the NIPP and are concluding a baseline risk assessment for the IT sector. We participate in the standards making process through international standards bodies. Many companies provide the products and services used to protect systems and networks, and they are innovating to do more. Many companies utilize those products and services in their own enterprise and in their enterprise solutions for customers including the Federal Government agencies. Additionally, discrete efforts are underway addressing software assurance and next generation response and security engineering.

All of these efforts rely on partnership between the public and private sectors. Together we do need to find ways to achieve wider adoption of solutions, standards, and best practices for greater overall security.

We commend the Congress for its early focus in this session on cybersecurity issues and this subcommittee for convening this panel today. We look forward to working with you. Again, thank you for the opportunity to appear today and express industry's perspective. I would be happy to answer any questions you may have.

[The prepared statement of Ms. Franz follows:]

TechAmerica
WHERE THE FUTURE BEGINS
THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

May 5, 2009

Written Statement

of

Liesyl I. Franz
Vice President for Information Security and Global Public Policy
TechAmerica

Before the

Subcommittee on Management, Organization, and Procurement
Committee on Oversight and Government Reform
U.S. House of Representatives

Chairwoman Watson, Ranking Member Bilbray, and distinguished members of the Subcommittee, my name is Liesyl Franz, and I am Vice President for Information Security and Global Public Policy at TechAmerica. Thank you for giving us the opportunity to testify today and to provide the technology industry's perspective on *Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems*.

TechAmerica is a trade association with the strongest advocacy voice for the technology industry in the U.S. formed by the January 2009 merger of four major technology industry associations – the Information Technology Association of America (ITAA), AeA (formerly the American Electronics Association), the Government Electronics and IT Association (GEIA), and the Cyber Security Industry Alliance (CSIA). The new entity brings together over 1500 member companies in an alliance that spans the grass roots – with operations in nearly every U.S. state – and the global – with relationships with over 70 national IT associations around the world. The U.S. technology industry is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. TechAmerica's members are the very companies – both hardware and software manufacturers – that serve as the foundation of our national digital infrastructure, as well as those that are providing systems integration services, enterprise IT and management solutions, and a wide variety of information security solutions for small, medium, and large companies, consumers, and government agencies.

I am here today to highlight the critical role of technology in helping to secure cyberspace – one we share with our government partners, our customers and users around the world. As products and service providers and critical infrastructure owners and operators, the private sector is a key stakeholder – and partner – in improving our cyber security posture. Technology cuts across all sectors of the economy – from financial services, telecommunications and the bulk of the electric power industry to critical government services – and the majority of the population relies on technology in their everyday lives. As such, we are mindful that security has to be built in from the very beginning and that we must continue to innovate aggressively in order to stay ahead of cyber criminals. We also see cyber security as a vital part of continuing economic growth and economic security, innovation, and U.S. competitiveness, as well as national and homeland security.

I will address the need for a national strategy under the auspices of a newly created position of Cyber Security Advisor in the White House, TechAmerica's continued call for improving the Federal Information Security Management Act of 2002 (FISMA), and the importance of the public private partnership and how it can be enhanced to address the challenges we face today and those we will face in the future.

Information Security Threats Continue to Evolve

First, let me characterize aspects of the current threat and vulnerability environment, based on reports from our members that monitor and address those threats and vulnerabilities every day. While specific attribution of an attacker is often elusive, we know that all manner of attackers are part of the threat picture, from individual hackers and spammers to fraudsters, from virtual criminal networks to established criminal organizations, and, reportedly, even nation states.

- According to Symantec Corporation's semi-annual *Global Internet Security Threat Report* published in April 2009, the key trend to note is that malicious activity is increasingly web-based. That means that attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers; instead, they are focused on attacking and compromising websites in order to mount additional, client-side attacks. Attacks can be more targeted, which makes it more efficient and effective for the attackers.

  Another notable trend is based on the increasing complexity of methods used by the attackers. For example, rather than only exploiting high-severity vulnerabilities, attackers are able to string together exploits for medium-severity vulnerabilities to achieve the same goal as exploiting a high-severity vulnerability. This means that organizations that only defend against exploits to high-severity vulnerabilities will miss some of these new multi-exploits.[1]

- The volume of cyber attacks continues to increase significantly. According to RSA's Anti-Fraud Command Center (AFCC), the volume of phishing attacks detected by RSA, The Security Division of EMC, grew an astonishing 66 percent over 2007.[2]

[1] *Symantec Global Internet Security Report: Trends for 2008;* Volume XIV, April 2009: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

[2] *RSA Anti-Fraud Command Center's 2008 Phishing Trends Report,* January 2009: http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1208.pdf

- Further demonstrating the evolution of cyber criminal behavior, Microsoft notes in its April 2009 Security Intelligence Report that the threat landscape in the U.S. was dominated by malware, which accounted for 67 percent of all exploits detected on infected computers in the second half of 2008. In addition, Microsoft also saw an increase in rogue security software infections of more than 48 percent compared with the first half of 2008.[3]

- In its 2009 trends analysis, McAfee notes the exploitation of web-based applications through social networking sites and consumer devices, as well as the growing distribution of malware in languages other than English.[4]

- According to Verizon's 2009 Data Breach Investigations Report, over 285 million records were compromised in 2008, and in 38 percent of those breaches, "malware" was utilized.[5]

- The challenges to securing federal systems are not only technological ones. In their recent report on *The 2009 State of Cybersecurity from a Federal CISO's Perspective*, (ISC)^2, Cisco, and Government Futures presented the results of a recent survey of agency Chief Information Security Officers (CISOs). They noted not only the external threat, but the insider threat as well.[6] In addition, while many CISOs feel they are more empowered today than they have been, many still cited bureaucratic constraints and staffing and resource concerns.[7]

These data points help illustrate the challenges that risk managers in both the private and public sector face in combating the growing sophistication, volume, and apparent success of a wide range of cyber attacks and information security breaches.

Organizing Effectively to Address the Information Security Challenge

The new Administration and the new Congress present an opportunity for a new National Strategy for Cyber Security that builds upon and enhances the work that has been done to date. We commend President Obama for calling for a White House 60-Day Review on cyber security, and we call on him to meet his campaign pledge to appoint a senior cyber security advisor in the White House.

I would like to emphasize two important points in this regard. The first is a fundamental issue regarding the synergy between cyber security and economic growth. As TechAmerica iterated in

[3] *Microsoft Security Intelligence Report*, Volume 6: July through December 2008: http://www.microsoft.com/protect/computer/SIR/Vol6.mspx

[4] McAfee White Paper: *2009 Trend Predictions: Slumping economy drives malware threats*: www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

[5] *2009 Data Breach Investigations Report: A study conducted by the Verizon Business Risk Team*; http://securityblog.verizonbusiness.com

[6] *2009 Data Breach Investigations Report:* 20 percent of the breaches investigated in 2008 were from insiders.

[7] *The 2009 State of Cybersecurity from the Federal CISO's Perspective – An (ISC)^2 Report*, April 2009

our response to the 60-Day Cyber Security Review, the relationship between security, prosperity, and innovation should be viewed and leveraged as a synergistic one.[8] In essence, in today's digital economy, information security contributes to the reliability of the critical infrastructure on which productivity and innovation depend, and the integration of security and privacy and civil liberties concerns engenders trust and confidence in the information infrastructure; by fostering reliability, trust, and confidence, security helps drives economic growth. In turn, a dynamic innovation economy drives an evolution in cyber security solutions that is critical to staying one step ahead of the threats.

Second, TechAmerica encourages the President to appoint a senior cyber official immediately. Doing so will provide a cyber security leader in the White House with the political leadership needed to develop and execute an updated national strategy to ensure coordinated, comprehensive, and effective implementation across the federal government and in partnership with industry. This first step is crucial to effective execution of the recommendations that may come out of the 60-Day Review.

As part of the public dialogue on cyber security, some have expressed concern that a new advisor in the White House would take authorities or responsibilities away from the Department of Homeland Security (DHS) or other agencies, but we do not believe that is the case. Certainly, DHS and other agencies will have a large role to play in providing strategy input and implementing key elements of it. For example, the U.S. Computer Emergency Readiness Team (US-CERT) plays an increasingly important role in protecting federal systems while working with the private sector to improve situational awareness, and those capabilities should be expanded. But, to date, there has not been an on-going, coordinated, national approach with senior White House leadership that would drive strategy development and cohesive implementation, bringing the strengths and capabilities of the various agencies and the concerns and input of stakeholders to bear. It is also important to note that such a position provides for a sustained voice in the White House for the cyber security component of issues of national concern.

Certainly an effective national strategy should include a strong focus on improving the security of federal information systems. TechAmerica (previously as ITAA) was a champion of FISMA when it was enacted in 2002, and we remain committed to the intent of the legislation. However, we do believe that in order to address the risk management challenges that federal agencies face today, FISMA needs to be updated to reflect the current organizational and operational environment. FISMA compliance grades may have improved over the years, but there does not seem to be a correlation between an agency's FISMA compliance and the state of its cyber security posture.

In 2007, TechAmerica testified before this Committee's Subcommittee on Information Policy, Census, and National Archives on FISMA and outlined six areas for update and improvement:

[8] *TechAmerica Response to the White House Cyber Security 60-Day Review:* http://www.techamerica.org/GovernmentAffairs/TechAmericaInput_CyberSecurity60_DayReview_FINAL.pdf

- Reform the annual agency information security program approval process
- Remove barriers to innovation
- Increase accountability
- Enhance federal cyber risk management
- Harmonize and enhance audit and oversight methods
- Expand federal cyber response capabilities.

We continue to advocate these areas for improvement, and we see many of them are being addressed in subsequent legislative proposals and in implementation. Of crucial importance is empowering the federal agency CISO and holding the agency leadership accountable for information security management.[9]

One specific area where important steps have been taken has been the implementation of the Office of Management and Budget's (OMB) guidance on Federal Desktop Core Configuration (FDCC) that set requirements for security settings for computers connected directly to federal agency networks. While we concur with the goals of the FDCC requirements, the process that was initially undertaken to promulgate the guidance did not include adequate consultation with industry. Subsequently, the National Institute for Standards and Technology (NIST) has invited vendors to participate in the development of standards for their products that would lead to appropriate requirements or controls. For any future engagement, we strongly encourage collaboration with industry partners from the beginning of the process to help articulate the problem and identify solutions. Such a collaborative process may require additional resources for NIST, which we believe should be considered and supported.

In order to effectively address the emerging threats, vulnerabilities, and challenges to federal information systems and, indeed, to our entire digital infrastructure, it is critical to engage in a public private partnership that is both strategic and operational.

On the strategic front, we have a partnership in place under the auspices of the National Infrastructure Protection Plan (NIPP), with its risk management framework for the 18 critical infrastructures and key resources, and the Critical Infrastructure Partnership Advisory Council (CIPAC). TechAmerica was instrumental in the establishment of the Information Technology Sector Coordinating Council (IT SCC), and I am honored to serve as the current Secretary. We have made strides in our risk management efforts for the sector, both in assessing our own risk and in working with the other sectors that depend on the products and services that our sector provides. The partnership has not been without its challenges, and there is always room for improvement, but we have organized ourselves well and continue to reach out to others to participate in our coordinated efforts.

Frankly, one early challenge was the government's own slow adoption of the NIPP framework as a partnership mechanism, except for discrete sector specific agencies like the National Cyber Security Division (NCSD) for the IT Sector and the National Communications System (NCS) for

[9] TechAmerica (ITAA) testimony before the Subcommittee on Information Policy, Census, and National Archives, June 2007: http://www.itaa.org/upload/news/docs/testimonybond060707.pdf

the Communications Sector, which have been committed to the NIPP partnership mechanism since the beginning. We do see increasing government engagement in the NIPP framework, but getting active agency participation in the Government Coordinating Council part of the partnership remains a challenge that needs to be addressed.

Also changing for the better is the federal government's improved outreach to the Sector Coordinating Council framework for input to strategic initiatives at the earliest possible point. Despite a rocky start, the SCCs were subsequently well-leveraged for input into Project 12, the critical infrastructure piece of the Comprehensive National Cyber Initiative (CNCI). The DHS Office of Cybersecurity and Communications has been an important part of that outreach. In addition, The White House reached out to the IT and Communications Sector Coordinating Councils as well as the NIPP's Cross Sector Cyber Security Working Group (CSCSWG) early in the consultative process for the 60-Day Cyber Security Review. We are seeing progress and more transparency in these processes, and we should insist upon even more collaboration along these lines.

Another strategic opportunity for public private partnership is in the area of research and development for greater cyber security into the future. While we are taking important steps in identifying where government and industry R&D is occurring and what the needs are, we have more to do in that area. In addition, we have yet to create a mechanism for true government-industry collaboration on specific projects. That will take some effort to define, fund, and implement, but it will be crucial for addressing longer term challenges and cyber security measures for the future.

A key element of the public private partnership is the operational component. The operational component is the day-to-day defense against, mitigation of, response to, analysis of, and recovery from cyber incidents in the broad eco-system. And, that component is made up of a series of relationships between operations centers and responders. To illustrate, both private and public enterprises often have network operation centers for cyber security, often referred to as Computer Security Incident Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs), or other similar entities. On occasion there are formal agreements for collaboration or information sharing between these CSIRTs, but for the most part, cooperation is informal or episodic. Relationships exist among the federal agency CSIRTs, among companies in Information Sharing and Analysis Centers (ISACs) and otherwise, between government and industry operations centers, and even among CSIRTs of all kinds (including government, industry, and academic) on a global basis in the Forum of Incident Response Security Teams (FIRST). The relationships are there and growing; we need to enhance and leverage them more fully, and we need to foster domestic and international collaboration and trust.

I will focus my comments here on the IT-ISAC, which serves as the operational focal point for the IT SCC.

The IT-ISAC is a trusted community of security specialists from companies across the IT industry dedicated to protecting the IT infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to

quickly and properly address them. The IT-ISAC's 24x7 Operations Center serves as a centralized hub for sharing information and providing analysis on threats and vulnerability information through secure communication channels.[10]
The notable elements of the IT ISAC are that it serves as an industry response and analysis center, and it provides a way for sharing information with – and from – the government. The IT ISAC works closely with the US-CERT which, in turn, provides a conduit for other government agencies. However, we can still improve upon that mechanism. US-CERT has improved its operational capabilities and processes over the past year, and the DHS Office of Cybersecurity and Communications should be commended for their efforts. However, the Department desperately needs an appropriate facility and more skilled manpower not only to manage the volume and complexity of incidents that are occurring, but also to take strategic steps to prevent them.

Ideally, we should build a joint industry/government operations center that includes a combined government watch center with, at a minimum, US-CERT and NCC/NCS and representation from each of the 18 critical infrastructures. Co-location would help to achieve productive, targeted, and purposeful information exchange and real-time analysis and collaboration between the government and industry. However, obstacles remain to co-location of analysts and responders from industry and government. Government has been reluctant to find ways to share actionable threat information with industry, and industry has not felt comfortable with government's ability to protect proprietary information. We have the opportunity to address those challenges and make change right now.

This is not to say that information exchange and cooperation does not occur. In a recent example, industry leaders galvanized their collaborative efforts around the Conficker worm. A "Conficker Working Group" was quickly established, and industry and government worked together on various aspects of the issue throughout its duration. The achievements and lessons learned from response to that incident could positively inform a path forward for collaboration that has predictable channels for communication and collaboration while maintaining the flexibility needed to address incidents on a case-by-case basis. In addition to providing its own independent analysis of Conficker, the IT-ISAC reached out to other critical infrastructure sectors and worked in tandem with other private sector organizations, such as the Financial Services ISAC, to raise awareness of the threat.

Lastly, I would also like to say a word about additional efforts underway in the private sector to address the challenges to securing critical infrastructure assets.

Industry is leveraging the partnership framework to facilitate collaborative efforts within and among sectors. For example, as part of its Sector Specific Plan (SSP), the IT Sector is completing an IT Sector Baseline Risk Assessment that evaluates risk to the IT Sector, focusing on the sector's critical IT Sector functions, rather than physical assets. The IT Sector's Baseline Risk Assessment is intended to provide an all-hazards risk profile that IT Sector partners can use to inform resource allocation for protection of the critical IT Sector functions and to serve as a baseline of national-level risk based on input received from subject matter experts from across

[10] http://www.it-isac.org

the IT Sector. While the assessment does not address all threat scenarios faced by IT Sector entities or their users and customers, it does address those operational or strategic risks to the IT Sector infrastructure that are of national concern. By increasing the awareness of risks across the public and private sector domains, the baseline risk assessment serves as a foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions.

The technology industry has been rapidly expanding its efforts to proactively address building security in to products, services, and platforms and to develop robust product assurance initiatives. Technology companies are strongly dedicated to increasing trust in information and communications technology products and services through:

- advancing effective assurance methods;[11]
- driving a new generation of security response and engineering;[12] and
- developing standards and best practices through participation in various standards making bodies and processes and leveraging those standards and best practices in their business operations and in the products and services they provide. We encourage the U.S. Government to engage more fully in the international standards making activities as well.

Conclusion

In sum, there are some key steps that can be taken to better secure government information systems. First, the Administration can act quickly to appoint a senior cyber security advisor with authority needed to develop, coordinate, and implement the President's cyber security priorities. Second, FISMA reform can enable and empower federal CISOs to understand their information security risks and take appropriate mitigation measures according to their organization's needs, including effective security controls that reduce exposure to a majority of vulnerabilities. Third, we can strengthen the public private partnership to address both strategic and operational concerns, both here at home and globally.

We commend the Congress for its early focus on cyber security issues and this subcommittee for convening this panel today. This congressional session provides a significant opportunity to make progress, and we look forward to working with you and your colleagues to develop proposals for meaningful change.

Thank you for the opportunity to appear before you today and express industry's perspective on this important issue. I would be happy to answer any questions you may have.

[11] One example of an industry group effort is the Software Assurance Forum for Excellence in Code (SAFECode), a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods: http://www.safecode.org.

[12] One example of an industry group effort is the Industry Consortium for Advancement of Security on the Internet (ICASI), which intends to be a trusted forum for addressing international, multi-product security challenges. This trusted forum extends the ability of information technology vendors to proactively address complex security issues and better protect enterprises, governments, and citizens, and the critical IT infrastructures that support them: http://www.icasi.org

Ms. WATSON. Thank you so much. I am going to throw out a question. I would like all the panelists to take part. It is similar to the one that I offered our first panel. How have the changes in technology such as the network architecture and the use of wireless devices and networks changed the approach that is needed for Federal cybersecurity?

Let me go on with the next one. Senator Rockefeller and Snowe recently introduced legislation that included provisions to establish a cybersecurity office in the White House along with Federal acquisition and procurement requirements for IT. These recommendations are also offered in the recent CSIS report for the new administration. I would welcome to hear from anyone that would like to address it first.

Mr. WILSHUSEN. I guess I will hit it off first. With regard to wireless security, increasingly the Federal Government is using that technology. We did a report back in 2005, I believe, which identified that Federal agencies had not taken sufficient steps to adequately secure the use of wireless security.

Obviously, there are some tremendous benefits that can accrue from using such technologies. It provides greater mobility and opportunities for individuals to perform services that they normally would not be able to do if they were tethered to a workstation at their desks. So clearly there are some benefits in using such technologies. But with the introduction of these types of technologies into the workplace, agencies need to assess the risk associated with those technologies and then take appropriate steps to mitigate those risks.

In our review, we found that they had not adequately done that. In many cases, they had not identified the types of vulnerabilities that such technologies would place, did not provide sufficient policies or procedures to mitigate those vulnerabilities, and did not take sufficient steps to train their staffs on how to appropriately and securely use these types of technologies.

So with the introduction of any new technologies, I would just say that there are some basic steps that need to occur in order to facilitate their secure use.

Mr. LEWIS. Thank you, Madam Chairman. One of the things that we have looked at in some of our work was who are the architects of the Federal Government. If you start looking at it a little bit, you find out it is people named Grover Cleveland and Herbert Hoover. This is good, but it is maybe time to modernize how Government operates a little bit. The question is how do we do that. One way to do that is to take advantage of the technologies you described. But as my colleague from GAO has said, when we take advantage of them—and we absolutely have to—we also have to think about security. Usually what happens is we do one and we don't do the other and then we are surprised. So I think it is essential to modernize but we need to do it in a secure fashion.

Mr. SACHS. Thank you. I think we are talking mostly technologies so we will get to Senator Rockefeller's bill in a moment.

Technology, of course, is something that our country has been a leader in since we started. There is no turning back there. The employees of the Federal Government are just like you and me and our kids and our grandparents, the people that are around us. We have most of these technologies at home. We want to bring them into work. The private sector has the same problem. So when new things come along such as wireless or handhelds or even new applications like the social networking sites, Twitter, Facebook, and things like that, there is naturally this desire to bring that back into the workspace, which could be the Federal Government or it could be the private sector.

We want to do the same thing at work as we do at home. That is a natural desire. Even with our cars, we would like to use that as the way to get around and not depend on having an office-provided or Government-provided vehicle that we have to wait in line for at a motor pool to have it available.

So our challenge then is as new technologies come along, as Mr. Lewis said, is that we have a unique situation with the Federal Government with the security of very sensitive information. These are the crown jewels of our Nation. These technologies make those crown jewels now exposed not just to local people but to the entire planet. This we have not faced before. Our adversaries can get into our hard drives remotely in a matter of milliseconds from virtually anywhere on the planet.

When we bring in new technologies, we bring in new exposures and new vulnerabilities, things we really haven't thought about. It takes a little while before we understand it, and after a while we begin to secure it. But our mindset needs to change. This is not the same as industrial technologies or new ways of doing aircraft or cars. These technologies are global and they expose us globally, literally within milliseconds.

So as long as we can grasp that and understand it, with that new mindset we can encourage employees to use the new technologies. But we have to show them how to use them so we don't put the Government's and our people's crown jewels at risk of being taken by our adversaries.

General RADUEGE. Thank you very much. I think it is interesting to point out that the intranet started in the Department of Defense not too many years ago. Of course, it grew into an Internet. Now the global community uses the benefits of that Internet and that way of communicating globally. We are stressing these days more and more open communications. We are more connected. Of course, we have become as a result more productive. We would describe this perhaps as entering an age of interdependence, though. We have become very dependent on each other for our world economies, our national securities, and our prosperities.

With more of these connections, though, and some estimate that by next year we will have 2 billion individuals and users connected to the Internet, we have become more vulnerable. Of course, the cyber criminals have found a new avenue for making money. It has become syndicated now. There has been an explosive growth of activity in cyber crime, as you are very well familiar. So with your first question about how the networks have changed, this is what we have seen. It has been exponential growth with exponential opportunity, but also the threats and vulnerabilities are very real.

Ms. WATSON. Ms. Franz.

Ms. FRANZ. I would just like to add the notion, to echo my colleague's comment, about technology being very exciting, very innovative, and contributing to the productivity, economic growth, and prosperity which retains our leadership in the global economy. However, new technology does provide challenges.

Industry is responding in many ways. One, we talked a lot about technology and training. We talked about empowering the user to use these technologies more securely. In addition, industry is increasingly baking security into its products and services. That is something that we heard a lot about in recent weeks during the RSA Conference in San Francisco in April, which is a great place to learn where some of these new technologies are going.

I think with regard to the Federal Government, though, one thing they can do is look at their procurement strategies and see if they can't be nimbler in adapting to the adoption of these new technologies not only for the benefits that they bring, but the security aspects that they bring as well.

Ms. WATSON. Thank you. I would like to go back to the GAO and Mr. Wilshusen. Recently, you completed work looking at the information security controls and practices at both the Los Alamos National Laboratory and the Tennessee Valley Authority. Can you cite some of the major information security control deficiencies in both studies? Are there similarities in the deficiencies of both entities? What are the challenges for them?

If you feel this is information that we don't need to share, then we will take it up in the classified section. But what can you tell us at this point?

Mr. WILSHUSEN. I can certainly address those issues I think at a high enough level where it won't be disruptive or compromising to the security at those organizations.

We have identified, as we do on most of our examinations of information security controls at agencies, a number of significant vulnerabilities at both the Los Alamos National Laboratory and at the TVA.

With regard to the TVA, we looked at the security controls and the network security controls over its corporate network as well as the networks supporting the control systems that operate key infrastructures operated by the Tennessee Valley Authority. We found a number of vulnerabilities related to controls that were insufficient to adequately identify and validate the identity of users in the access privileges granted to those users.

We found weaknesses with regard to the firewalls that were in place at those organizations, which could allow certain firewalls to either be bypassed or not adequately segregate and prevent network traffic that should not be passed through those devises.

We also found a number of problems associated with their auditing and monitoring capabilities. Those are the controls which agencies use to try to identify, detect, and then respond to unauthorized traffic or security incidents.

So we find pretty much weaknesses in most of the general control areas that we look at. We found those at both Los Alamos and at TVA.

With respect to TVA, we found not only the cybersecurity related weaknesses but also physical security weaknesses as well. Combined with the cybersecurity weaknesses that we identified, these placed the control systems and networks that we examined at risk to both internal and external threats.

Ms. WATSON. Well, some have made the case that our military agencies have better technical and organizational capabilities for addressing cybersecurity in the Federal Government when compared with the multiple operational layers of DHS. Can you comment on whether DHS has adequate or similar capabilities for operational cybersecurity?

Mr. WILSHUSEN. As you may know, back in 2003 President Bush issued the National Strategy to Secure Cyberspace. As part of that strategy, DHS was the focal point for much of the Federal cybersecurity efforts.

Over the past several years, GAO has identified and consistently reported that DHS has not consistently implemented or met those responsibilities. In total, we issued about 30 recommendations on various different core elements related to protecting cybersecurity. As a result, we have found that DHS has just not adequately performed their responsibilities for a number of different reasons, not the least of which is the significant turnover in their leadership and key personnel positions in the cybersecurity area.

Ms. WATSON. I just thought the agency was too big. Putting them all under one roof, when you have had the experience of being the master of your unit and now you have to report to someone else, it just wasn't going to work out all that efficiently.

But let me hear from the rest of you. We will just go down the line.

Mr. LEWIS. This is a serious problem and it is not going to be easy to fix. We would all prefer that it be a civilian agency. Everyone thought it should be DHS. But as my colleagues have said, they are not yet capable of performing the mission. So one of the questions you want to ask is how long do you want to wait. Depending on who you talk to, they say DHS could be ready in 3 years or 5 years or 10 years. We can't wait 3 or 5 years.

The dilemma is the only place that really has the capability now is the Department of Defense, particularly the National Security Agency. But when you say that, you immediately trigger Constitutional concerns. You trigger the memory of the FISA debate. We have a problem. The people who could do this best are in the intelligence community, but we are not comfortable with that. The people who would be the civilian focal point for this aren't ready or capable.

So how do we fix that problem? That is a very difficult issue and it is one I think we are going to have to wrestle with for the next couple of years.

Mr. SACHS. As one of the guys that was there when we opened the doors for DHS in the spring and summer of 2003, we had a lot of euphoria about what we could do. We had this beautiful charter in front of us and the pasture was green. We look back on those days now, and I see Mr. Lewis chuckling.

The summer of 2003 was when the Blaster Worm hit. There were outages in the power sector. I am sure we all recall that. When the agency was young, still maybe she had a lot of naivete about it, but we did quite well because we didn't know what we couldn't do or what we weren't supposed to do.

Unfortunately, in my opinion, what has happened over the years is the agency has been unable to grow in the manner that we were hoping that it would. It has been unable to take on the challenges and the responsibilities that we hoped it would. There have been a lot of politics surrounding them, as you are aware. There has been a lot of media scrutiny. There has been a lot of private sector scrutiny and international scrutiny. DHS is very big. It encompasses parts of 24 different Federal agencies that were pulled together. There is a culture that has to be stitched in. Underlying all of this, of course, is cyberspace, this thing that we are all very familiar with. And they have the role of making it secure.

I don't envy my counterparts at DHS. This is a tough mission that they have in front of them. They have very good people that are there but they are constrained by a lot of things that are beyond their control. I think one of the best things we could do is really get out of their way and let them, particularly in cyberspace, let them do what they need to do. Give them the latitude, the ability to grow, the ability to hire the right people, and let those people run. Give them the pasture and let them do what they need to do.

I believe the private sector is more than willing to work with DHS. Many of us do spend our days over at the Department. We have some very strong public/private bonds that have been built over the years. We all do want to make this work.

A key to all of this is leadership. We need to get some good appointments. We need to get strong people, people who are dedicated in service to their country and are willing to be there year after year, people that we in industry are willing to work with. I think we can do that.

I have a lot of optimism for the Department and I do look forward in the next coming years or so to seeing big changes there.

But just to go back to the military because I spent 20 years there. The military has a very old culture. We have to recognize that. It has been around over 200 years. DHS is only 6 years old. We cannot expect DHS to perform like a 200 year old department. It just is not there yet. So patience, I beg of you. We will get there with them.

General RADUEGE. Madam Chair, I come from a military background, as you noted earlier, having spent 35 years on active duty. I was serving during the time in 1998 when in the Department of Defense we recognized the fact that our computers were being attacked. So the responsibility was given to the U.S. Space Command at that time to create some sort of a program to defend our computer networks. I was privileged to serve at that time within the U.S. Space Command. The program we put together in 1998 has grown over the years to now what is considered by many to be a very outstanding program.

The Department of Defense also has the benefit of a command and control system and network where individuals work for each person. You know exactly who you work for. There are orders that can be given and they have to be followed based on the requirements of the Uniform Code of Military Justice. That is what the command and control of the Department of Defense is all about. Our other organizations, though, don't have that kind of a structure.

I would point out that in my years, now over a decade of working with this area that initially was called computer network defense and now has gone into a cybersecurity type of terminology, that there are a number of departments in our Federal Government that have key roles in this. I would just point out the Department of Homeland Security, the Department of Defense, the intelligence community, the Department of State, the Department of Commerce, the Department of Justice, and the Department of Interior just to mention a few that have key roles in a national strategy for securing cyberspace.

I believe it is for that reason, the realization that someone had to be in control of that and have some sort of oversight, and for that reason—I was proud to serve with our Center for Strategic and International Studies Cybersecurity Commission—we recommend that we consider an individual in the White House that would have the opportunity to create policy and to provide oversight and a balanced Federal program across all the Federal departments and agencies. We feel like that is a critical way to have someone in charge to move us forward in this critical area.

Ms. WATSON. Thank you.

Ms. Franz.

Ms. FRANZ. Thank you. I don't have much to add to the very good comments of my fellow witnesses except probably to put things slightly in perspective with regard to the relationship between DHS and DOD. We should remember that DHS had very limited resources both from a staffing perspective and from a funding perspective in its early days. Since the beginning, it has leveraged the manpower of DOD and the systems and strategies that had been used in DOD. So that has been a positive impact, I would say.

But it does need to be its own entity. It has a different mission. It has a different perimeter and parameters than the Department of Defense has. So it does need to build its own manpower. Importantly as well, it really needs its own facilities that provide it a base of operations. That has been a challenge since the very beginning. It was a challenge when I was there in the National Cybersecurity Division and it remains a challenge today.

DOD has a more impressive facility and a capable one. That should be no surprise given the funding differences between the two. So resources, manpower, and facilities are really key to making some improvements soon.

Ms. WATSON. I want to go back to Mr. Lewis again. I think the other panelists have been addressing this issue. But as part of the CNCI, there is an ongoing debate as to what role the DHS ought to have as a leading agency charged to coordinate and respond to cyber related incidents.

I wish they would have been here today to answer these questions. But do you think, and I think many of you have commented on it already, does DHS have the technical or operational capabilities to be in charge of handling cyber?

Mr. LEWIS. Well, you have heard some of the answer earlier. They have a really good team there now. There are some really good folks. That is an improvement. They do have a shortage of resources, facilities, trained folks, and money. It is hard to believe after all these years, but they are not equipped.

I was talking to someone who was over at DHS Cyber Division last week and they said the staffing is running at about 30 percent. So for every one person who is there, there are two who are missing. I don't know if that is right. This is what I was told. But I have heard repeatedly from many people that severe resource problems put them at a disadvantage. They don't have the trained people.

Now, they do have a very important mission. The NCSD, the National Cybersecurity Division, should be the place responsible for securing the .gov networks. It has to work with critical infrastructure. It has to work with the private sector. That is enough, particularly when they aren't staffed or funded. They don't need to pick up more missions. But the missions they have are really important and we should hopefully make them capable of carrying them out.

As I say, though, there is a great team there now. It is probably the best team they have had in a long time. So there is a chance.

Ms. WATSON. Let us hope. I want to go to you, Mr. Sachs. From your Government experience which dates back to the Clinton administration's 1998 Presidential Directive for securing critical infrastructure sectors, what are the so called lessons learned that the Federal Government has improved upon over the past decade? Conversely, where are we not learning? What are we not learning from our mistakes?

Mr. SACHS. The middle 1990's, the concern was one of the critical infrastructures. We saw .com growing. We knew that Russian bank robbers were breaking in. The Air Force had intrusions at Roane [phonetic] Laboratory. There was this understanding that the Internet, while great, was offering these new problems that we really didn't know how to get our hands around.

The bombing of Oklahoma City in 1995 was the big eye opener. Not only were children and people killed there, but we had quite a few Government computer systems in that building that were destroyed when that bomb went off. We found within minutes that several Government department data bases literally weren't there. They had chosen that building because they thought physically it was in the middle of nowhere. Nobody was going to attack it. It was far, far away from Washington and New York City and places a terrorist would go after. They realized that this linkage between physical and cyber was more than just science fiction; it really did exist. A terrorist attack doing something physical could have an effect in cyberspace. So that set forth a series of congressional hearings and White House investigations. DOD and others got involved.

There was an exercise in 1997, highly classified at the time but today we can read all about it, called Eligible Receiver. It showed that portions of the Defense Department's networks could be reached from the civilian networks, from home. Literally, I could dial into the Internet and gain access to classified computers. We were that porous back in the 1990's. So a lot has come since then.

As General Raduege mentioned, the JTF-CND was created in 1998 as part of that. I was part of that group also that stood that up. We immediately took upon ourselves to secure the Defense Department, not North American cyberspace. This wasn't like a NORAD for the Internet. But even just looking at DOD, we found we were extremely porous. We had Web sites that listed flight schedules for Generals. We had Web sites that showed full bunker maps of all the nuclear facilities. I mean, it was unbelievable what information we were making available to our adversaries. That was on unclassified Web sites, not even talking about access to what we thought was classified.

So since then, I think the big lesson that has been learned is that information seeks to be free. If you put information somewhere, if you put it on a hard drive, doggonit it will attempt even on its own to leak out. But we make it easy. We connect sensitive computers to the wide open Internet. We allow our employees to swap files back and forth. We don't train them. We don't teach our employees, both in the private sector as well as Government, the danger of cross-connections. The actual information is ones and zeros that are on hard drives, but we don't teach them how much risk that can put our Nation against.

Our adversaries on the other hand understand this game fully. The Chinese in the late 1990's published their doctrine of unrestricted warfare. Many of us read it; looked at it; and said yes, they got it. They understand it. We looked at ourselves and our doctrines and policies didn't even come close. In our arrogance, because we invented the Internet and everything speaks English online, we were thinking that this is ours and we can control it. But they understood it. We are seeing this today. This has now come back around to bite us.

So this is our challenge going forward, as we look back at the 1990's and as we look at this decade as it comes to an end here in a few months. We have learned so much about cyber crime, cyber espionage, military actions online, and even just what people want to do and what society wants to do with the networks. So as we go forward, 2010 and the years beyond, the Internet doesn't go away. Cyberspace doesn't go away. It is really just part of what we are.

I think the Federal Government, in a partnership with the private sector and with America, has to face this challenge head on. We take the Internet as what it is. It is an economic engine. It is the fuel for recovery. It is exactly what we need to stimulate us, to use some of the terms that have been used here. We must protect it. We must guard it like that and think about it economically. Otherwise, we lose and we lose big. Our adversaries, again, they understand this game and they are able to think in front of us.

Ms. WATSON. Let me get to General Raduege. It seems to me, and I think we have all mentioned this, that the Federal Government has too many cooks in the kitchen for cyber coordination and organization. This is a fair assessment. I think all of you have been saying that. As the former head of DISA, could you offer up some thoughts on where the Government could improve its organizational hierarchy for cybersecurity across the entire agency community?

General RADUEGE. Madam Chair, as I mentioned, I think we need to have someone at the top of this hierarchy of our Nation that can give the proper guidance and policy, the proper oversight, and can lead from the top in putting together a comprehensive approach to addressing cyberspace and what it means to us in our future.

I also wanted to comment on the fact that this doesn't require cyber science. It boils down a lot also to management techniques and policies. For example, a lot of computers are broken into through electronic means. But we also don't have the proper governance, the proper policies and procedures in managing our capabilities when people steal laptops from our vehicles, steal them from our cars, or when we just lose our computer capabilities. So a lot of this also boils down to policies and procedures of managing the capabilities. In many cases, we are just too careless with our cyber equipment.

So I would state that as something that we need to develop additional governance around and better procedures. This gets back to the part about the education and awareness, and developing a cyber mindset. We just don't realize how vulnerable we are to just someone picking and choosing the computers that we allow access to on a daily basis.

I can tell you that the organization that I am with now in civilian life stresses this with every employee all the time. So now when I travel, I think twice when I am in my hotel room. I never leave my hotel room and allow my computer to stay there. As a matter of fact, I don't even lock it in those little safes they provide. I carry that computer around with me on my person at all times because in the organization I am with, our name is our reputation. To lose a computer to someone who steals it would be devastating to our business opportunities. So it is something that we have stressed in our education process.

Ms. WATSON. Let me just ask, do you have a backup? Could you put a chip in there so you will know, so it will signal you wherever it is? Would you not have a backup to what you have on your computer?

General RADUEGE. I have backups to what is on my computer but I want to make sure that unauthorized individuals don't gain access to my computer and the networks that I am authorized to operate in.

Ms. WATSON. Well, couldn't a chip signal you some way that it is out of your control? If your computer is not with you, could it signal you so you could turn it off or destroy what is on there or black it out? It seems that we have technology that would work that way.

General RADUEGE. We have a lot of technology and a lot of technology could be put into place that would have that kind of a capability. But most individuals I don't think operate in that fashion today. So it is a very manual process of controlling the asset that is in your possession.

Ms. WATSON. Let us go to Ms. Franz now. There seems to be a significant amount of resistance from industry regarding policy proposals that would establish standards for information security controls and software assurance for Government systems. Can you explain this to me, why there is this resistance?

Ms. FRANZ. Certainly. I am not sure I would characterize it as resistance from the industry to discuss the kinds of things that may be needed to address specific issues and specific problems. As

I mentioned in my remarks, the industry is involved in standard making processes in international standards making bodies. They see a benefit to standards for both interoperability and for security concerns.

I think the issue is around proposals that may come that are trying to address some of the problems but don't do so either in a targeted way or in a consultative way with industry, the way we see it happen in those exchanges in the international standard making bodies, for example. So I wouldn't say it is a resistance to identifying clear needs and then taking steps in a partnership fashion, in a consultative fashion to find out the best way to address those needs.

There can always be unintended consequences from either regulation or standards or, dare I say, even legislation that may have a broad brush and not address the concern specifically. It can have unintended consequences for the impact on industry and consumers and Government users, for example.

Ms. WATSON. I would like to have each one of you give us one concluding statement that you feel will help us. We are going to be making recommendations. We might have a bill; we might just make some strong recommendations to the executive branch. But what would your last input be that you think would be helpful? Let us start with the GAO.

Mr. WILSHUSEN. I think I would suggest that you ensure that in your bill you establish mechanisms for establishing accountability over the actions that agencies need to take. Assure that they are held to task to implement those particular requirements, whatever you may include in your bill. I think accountability is key. That would be my one remark.

Ms. WATSON. Mr. Lewis.

Mr. LEWIS. Thank you. I would say we need to come up with a plan. We need to put the White House in charge of that plan and we need to get moving on it. We have been doing this now for 10 years and we are worse than when we started.

On the accountability note, I think one thing that Congress can do, and one thing that legislation can certainly do, is you have the authority and the oversight responsibility to hold Government and the private sector accountable for when there are lapses. There certainly have been enough lapses in the last few years.

Mr. SACHS. I would like to also highlight the people. I think this is the real angle that could make a very good nucleus of anything in the future. There are three groups that really make all of this work.

There are Government officials and people who work within the Government. They know each other; they are very professional.

There is the private sector. I am talking about the private sector that is profit oriented, that do the work. They run the carriers and so forth.

Then there is this third group of volunteers who are the unsung heros, the ones that collaborate. This Conficker Worm that was going around recently largely was solved by a volunteer effort that has come together. There was no formal approach toward that leadership. We have seen this over the years that this type of problem solving tends to just come out of nowhere by the volunteers. So they are very important, those three groups. But I highlight that because of the people piece.

In cybersecurity, the professionals like myself and the rest of the panel here who do what we do, we still need to have our profession professionalized. You will see this called for in the CSIS report. I believe Senator Rockefeller has it in his bill, the notion that says that those who are professional in this world need to become professional. We need to be certified; we need to be licensed.

It is more than just passing an exam but actually licensed and bonded. We do this with real estate sales people. We do it with people who groom dogs. We do it with lawyers and countless other professions. Right now, the essence of our Nation, trillions of dollars of value, is being managed by very good people but we don't have a licensing or a licensed profession.

Now, we don't solve that overnight. This may take years. The profession needs to do it ourselves. But it would be helpful if the Congress would think about how to enable that, how to help the profession become professional.

Ms. WATSON. Thank you for that input. General.

General RADUEGE. Madam Chair, I would say for one point that is different than those already expressed, that I would stress the fact that we could significantly improve Federal cybersecurity by operationalizing the intent of the FISMA legislation. By doing that, we would also use performance based measurements for security so that we really are measuring the operation of security throughout our Federal networks instead of just an audit of the checklist.

Ms. WATSON. Thank you.

Ms. Franz.

Ms. FRANZ. I think I would like to respond to your comment about too many cooks in the kitchen. I wouldn't want to leave the impression that we have too many people working on cybersecurity these days because I don't think any of us would agree that is the case.

However, we don't have a head chef. Let us create a head chef. Let us empower the cooks in each of the agencies, or their kitchens, to do their jobs. Let us give them empowerment before we measure them. Then let us look at making changes that enable rather than prohibit the partnership to really operate the way that it could in a shared environment.

Ms. WATSON. I think I have heard over and over, General, that you need somebody to head up the Joint Chiefs of Staff.

I think your input has been very, very valuable to us. We have it all recorded. We have your reports. We will be reaching out to you again. With your statements, we are going to adjourn this meeting but we will be back in touch. Thank you so much for your testimony.

The meeting is adjourned without objection.

[Whereupon, at 5:10 p.m., the subcommittee was adjourned.]

○